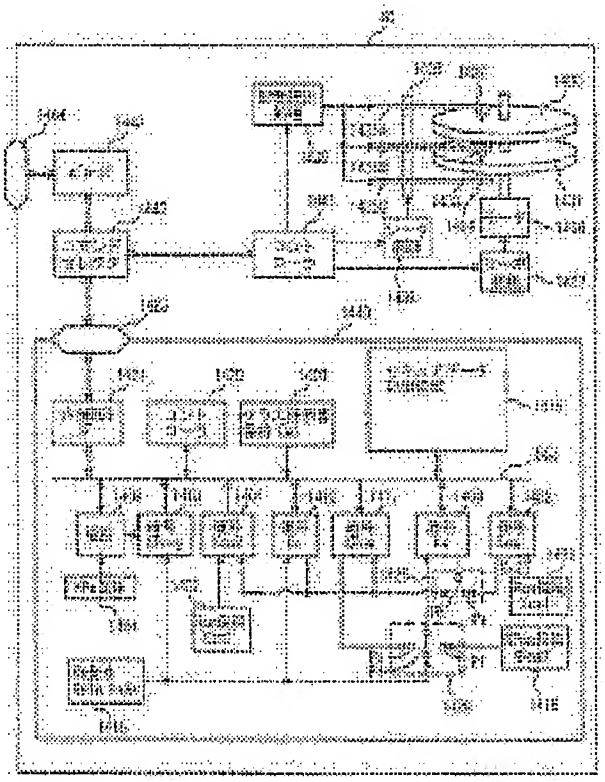
HARD DISK UNIT

Publication number: JP2003248557 (A)
Publication date: 2003-09-05
Inventor(s): HORI YOSHIHIRO; HIOKI TOSHIAKI
Applicant(s): SANYO ELECTRIC CO
Classification:
- international: ***G06F12/14; G06F3/06; G06F21/24; G09C1/00; G11B19/12; G11B20/00; G11B20/10; G11B20/12;*** *G11B5/012;* **G06F12/14; G06F3/06; G06F21/00; G09C1/00; G11B19/12; G11B20/00; G11B20/10; G11B20/12;** G11B5/012; (IPC1-7): G06F3/06; G06F12/14; G09C1/00; G11B20/10; G11B20/12
- European: G11B19/12C; G11B20/00P; G11B20/10
Application number: JP20020049763 20020226
Priority number(s): JP20020049763 20020226

Also published as:
US2003161064 (A1)
CN1441590 (A)

Abstract of **JP 2003248557 (A)**

PROBLEM TO BE SOLVED: To provide a hard disk unit capable of fully protecting confidential data. ; SOLUTION: A hard disk unit 40 stores encrypted contents data into hard disks 1430 and 1431 by a storage reading processing part 1439 and a license for decoding the contents data is stored into a secure data area 1415 in a storage element 1440. The storage element 1440 is composed of semiconductor elements, and hard disk units 40 and 41 are accessible independently. ; COPYRIGHT: (C) 2003,JPO



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－248557
（P2003－248557A）
(43)公開日　平成15年９月５日(2003.9.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｍ	５Ｂ０１７
12/14	３２０	12/14	３２０Ｂ	５Ｂ０６５
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｄ	５Ｊ１０４
			Ｈ	

審査請求　未請求　請求項の数５　ＯＬ　（全 30 頁）　最終頁に続く

(21)出願番号　特願2002－49763(P2002－49763)

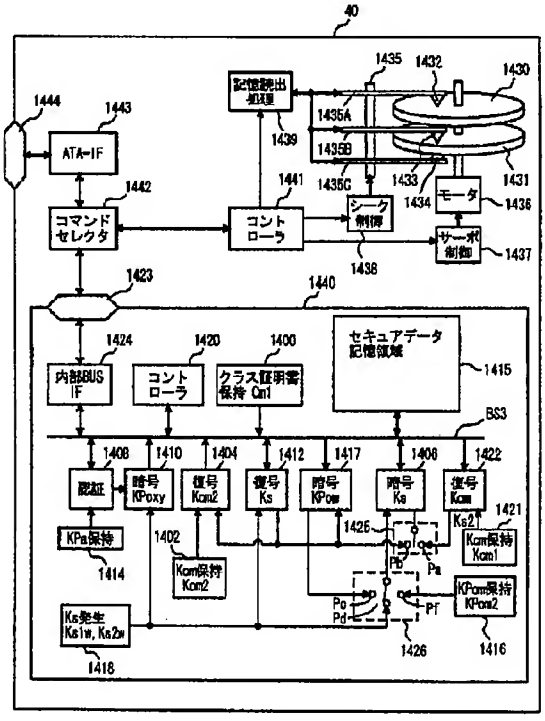
(22)出願日　平成14年２月26日(2002.2.26)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　日置　敏昭
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　ハードディスクユニット

(57)【要約】
【課題】　機密データを十分に保護可能なハードディスクユニットを提供する。
【解決手段】　ハードディスクユニット４０においては、暗号化コンテンツデータは、記憶読出処理部１４３９によってハードディスク１４３０，１４３１に記憶され、暗号化コンテンツデータを復号するためのライセンスは記憶素子１４４０のセキュアデータ記憶領域１４１５に記憶される。そして、記憶素子１４４０は半導体素子として構成され、ハードディスクユニット４０，４１とは独立してアクセス可能である。



1

【特許請求の範囲】

【請求項１】　機密データと非機密データとの入出力を行ない、かつ、前記機密データと前記非機密データとを記憶するハードディスクユニットであって、
外部とのデータの授受を行なうインタフェースと、
外部の他の装置とデータをやり取りする端子と、
前記端子を前記インタフェースに接続するデータバスと、
前記機密データを記憶し、不正なアクセスから前記機密データを保護する記憶素子と、
前記非機密データを記憶する円盤状磁気記憶媒体と、
前記非機密データを前記円盤状磁気記憶媒体に記憶および／または読出を行なう記憶読出処理部とを備え、
前記記憶素子は、
前記機密データを記憶するデータ記憶部と、
前記機密データを入出力する場合に、前記機密データの提供元または提供先との間で暗号路を構築し、かつ、機密データの入出力を関するデータ管理部とを含む、ハードディスクユニット。

【請求項２】　前記記憶素子は、独立した半導体素子によって構成される、請求項１に記載のハードディスクユニット。

【請求項３】　前記記憶素子は、当該ハードディスクユニットから着脱可能である、請求項１または請求項２に記載のハードディスクユニット。

【請求項４】　前記機密データの入出力処理に関するデータの授受を前記インタフェースと前記記憶素子との間で仲介し、前記非機密データの入出力処理に関するデータの授受を前記インタフェースと前記記憶読出処理部の間で仲介する選択部をさらに備える、請求項１から請求項３のいずれか１項に記載のハードディスクユニット。

【請求項５】　前記インタフェースは、
前記機密データを外部との間で授受する第１のインタフェースと、
前記非機密データを外部との間で授受するための第２のインタフェースとを含み、
前記端子は、
前記他の装置とデータをやり取りする第１の端子と、
前記第１の端子を前記第１のインタフェースに接続する第１のデータバスと、
前記他の装置とデータをやり取りする前記第１の端子から独立した第２の端子と、
前記第２の端子を前記第２のインタフェースに接続する第２のデータバスとを含む、請求項１から請求項４のいずれか１項に記載のハードディスクユニット。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶するハードディスクユニットに関し、特に、マルチアクセスが可能な記憶装置においてコピーされた情報に対する著作権保護を可能とするハードディスクユニットに関するものである。

2

【０００２】

【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００７】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【０００８】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセ

3

ンスを識別するためのライセンスＩＤ、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築する。

【０００９】最終的に、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

【００１０】メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

【００１１】また、メモリカードは、他のメモリカードとの間でライセンスの移動または複製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

【００１２】このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。

【００１３】また、近年、放送網のデジタル化、デジタル通信路の広帯域化によって大量なデータの送信が可能となりつつある。このようなデータ送信環境の変化によって、これまで、音楽データのように比較的データ量の少ないコンテンツデータから、大容量な映像データの配信を行なうことができるインフラストラクチャーが整いつつある。

【００１４】一方、メモリカードは、映像データを扱う場合には、データ記憶容量が少ない、データのアクセス速度の遅いデータに対する１ビット当りの記憶単価が高いなどの性能・価格の面から見ると、映像データを扱うには最適な記憶メディアであるとは言い難い。

【００１５】大記憶容量、高速アクセス、かつ、１ビット当りの記憶単価が安い記憶メディアとしてハードディスクユニットが存在する。

【００１６】

4

【発明が解決しようとする課題】しかし、現行のハードディスクユニットは、ライセンスのような機密性を要する機密データを記憶する媒体としては、その機密性が低いという問題がある。

【００１７】また、ハードディスクユニットは、内部にモータなどの能動部品を備えているために装置寿命が短いこと、耐衝撃性が低く、ユニット内部に備えられている磁気記録媒体であるハードディスクユニットの損傷によってハードディスクユニット上の記憶されたデータが容易にアクセス不能となることから明らかなように、ライセンスのようにバックアップを取ることが許されないデータそのもの価値のある機密データを扱うには、記憶の安全性が低いという問題もある。

【００１８】そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、ハードディスクのように記憶されたデータが読出不能となった場合でも、記憶されている機密データに対するアクセスを保証し、機密データに関する記憶の安全性を確保するハードディスクユニットを提供することである。

【００１９】

【課題を解決するための手段】この発明によれば、ハードディスクユニットは、機密データと非機密データとの入出力を行ない、かつ、機密データと非機密データとを記憶するハードディスクユニットであって、外部とのデータの授受を行なうインタフェースと、外部の他の装置とデータをやり取りする端子と、端子をインタフェースに接続するデータバスと、機密データを記憶し、不正なアクセスから機密データを保護する記憶素子と、非機密データを記憶する円盤状磁気記憶媒体と、非機密データを円盤状磁気記憶媒体に記憶および／または読出を行なう記憶読出処理部とを備え、記憶素子は、機密データを記憶するデータ記憶部と、機密データを入出力する場合に、機密データの提供元または提供先との間で暗号路を構築し、かつ、機密データの入出力を関するデータ管理部とを含む。

【００２０】好ましくは、記憶素子は、独立した半導体素子によって構成される。好ましくは、記憶素子は、当該ハードディスクユニットから着脱可能である。

【００２１】好ましくは、ハードディスクユニットは、機密データの入出力処理に関するデータの授受をインタフェースと記憶素子との間で仲介し、非機密データの入出力処理に関するデータの授受をインタフェースと記憶読出処理部の間で仲介する選択部をさらに備える。

【００２２】好ましくは、インタフェースは、機密データを外部との間で授受する第１のインタフェースと、非機密データを外部との間で授受するための第２のインタフェースとを含み、端子は、他の装置とデータをやり取りする第１の端子と、第１の端子を第１のインタフェースに接続する第１のデータバスと、他の装置とデータをやり取りする第１の端子から独立した第２の端子と、第

２の端子を第２のインタフェースに接続する第２のデータバスとを含む。

【００２３】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２４】図１は、本発明によるデータ保護機能を備えたハードディスクユニットに対して、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するライセンスを記憶するための構成を示した概略図である。

【００２５】コンテンツ提供装置３０は、ハードディスクユニット４０に記録する暗号化コンテンツデータおよびライセンスを提供する装置であり、データバスＢＳを介してハードディスクユニット４０と接続され、データバスＢＳを介してデータの授受を行なえる構成となっている。

【００２６】なお、以下では、デジタル通信網、たとえば、インターネットを介して映像データをダウンロードしてハードディスクユニット４０に記録する配信システムを例にとって説明するが、以下の説明から明らかなように、本発明は、このような場合に限定されることなく、生データを取り込んで暗号化コンテンツデータおよびライセンスを生成し、その生成した暗号化コンテンツデータおよびライセンスをハードディスクユニット４０に記憶するデータレコーダや、放送網を介して受信した暗号化コンテンツデータやライセンスをハードディスクユニット４０に記憶する放送受信システム、放送網を介して暗号化コンテンツデータを取得し、デジタル通信網を介してライセンスを取得する複合配信システムなど様々な構成が考えられる。すなわち、コンテンツ提供装置３０は、暗号化コンテンツデータおよびライセンスの取得経路に限定されることなく、ハードディスクユニット４０との間で、データの授受を行ない、暗号化コンテンツデータとライセンスとをハードディスクユニットに送信する機能を備えている装置である。

【００２７】また、映像データに限定されることなく、他の著作物としてのコンテンツデータ、たとえば、音楽データ、画像データ、朗読データ、テキストデータ、コンピュータプログラム、ゲームソフトなどを扱うことも可能なものである。

【００２８】図１を参照して、データ配信システムにおいては、コンテンツ提供装置３０は、ダウンロードサーバ１０と端末装置２０によって構成される。ハードディスクユニット４０は、脱着可能なコネクタを備えた独立したユニットである。データバスＢＳは、端末装置２０は、ハードディスクユニット４０を装着する機構を介して接続可能なデータバスである。また、端末装置２０は、デジタル通信網を介してコンテンツの配信を行なうダウンロードサーバ１０と接続されている。

【００２９】ダウンロードサーバ１０は、ハードディスクユニット４０を装着した端末装置２０のユーザからの配信リクエストを端末装置２０から受信する。映像データを管理するダウンロードサーバ１０は、配信リクエストを送信してきた端末装置２０に装着されたハードディスクユニット４０が正当な証明書を持つか否か、すなわち、保護機能を備えた正規の記憶装置であるか否かの認証処理を行なう。そして、ハードディスクユニット４０が正規のハードディスクユニットであった場合、ダウンロードサーバ１０は、ハードディスクユニット４０に対して著作権を保護するために所定の暗号方式により映像データ（以下、「コンテンツデータ」とも呼ぶ。）を暗号化した暗号化コンテンツデータと、このような暗号化コンテンツデータを復号するためのコンテンツ鍵を含むライセンスとを端末装置２０へ配信する。

【００３０】端末装置２０は、配信された暗号化コンテンツデータとライセンスを、ハードディスクユニット４０に記憶するためにダウンロードサーバ１０とハードディスクユニット４０との仲介処理を行なう。

【００３１】このとき、ライセンスの配信についてはダウンロードサーバ１０とハードディスクユニット４０との間にはセキュアコネクション（暗号通信路）が形成され、その中をライセンスが配信される。すなわち、ライセンスは、ハードディスクユニット４０においてのみ、復号可能な暗号化が行なわれて配信され、ハードディスクユニット４０において復号され、記憶される。セキュアコネクションの形成については後に詳細に説明する。このようなライセンスをハードディスクユニット４０へ記憶する処理を「書込」と称することとする。

【００３２】さらに、端末装置２０に再生機能を備えれば、ハードディスクユニット４０に記憶された暗号化コンテンツデータとそのライセンスを読出して再生することが可能である。図２は、端末装置２０が再生機能を備え、ハードディスクユニット４０に記憶された暗号化コンテンツデータとそのライセンスを読出して再生するための構成を示した概略ブロック図である。

【００３３】図２を参照して、端末装置２０は、端末装置内部の制御およびデータバスＢＳを介したハードディスクユニット４０とのデータの送受信を制御するコントローラ１１０６と、暗号化コンテンツデータとライセンスによってコンテンツの再生を行なうデータ保護機能を備えた再生回路１５５０によって構成される。コンテンツの再生時においても、ハードディスクユニット４０と再生回路１５５０との間にはセキュアコネクションが形成され、その中を再生に使用されるライセンスがハードディスクユニット４０から再生回路１５５０に送信される。このとき、ハードディスクユニット４０において再生回路１５５０の正当性の確認が再生回路１５５０の証明書の認証処理によって行なわれる。再生回路１５５０に対してコンテンツ鍵を送信し、暗号化コンテンツデータの再生に備える処理を「使用許諾」と称することとす

る。詳細については後述する。

【００３４】さらに、ダウンロードサーバ１０から受信し、ハードディスクユニット４０に記憶された暗号化コンテンツデータおよびライセンスは、他のハードディスクユニットへ送信することもできる。図３は、端末装置２０に備えられたデータバスＢＳに２台のハードディスクユニットを接続したハードディスクユニット間での暗号化コンテンツデータおよびライセンスの送信をするための構成を示した概略ブロック図である。

【００３５】ハードディスクユニット４０と同一の機能を備えるハードディスクユニット４１が、データバスＢＳに接続されている。端末装置２０のコントローラは、２つのハードディスクユニット４０，４１間のデータの送受信の制御とデータの仲介とを行なう。また、ライセンスの送信に当っては、ハードディスクユニット４０とハードディスクユニット４１との間にはセキュアコネクションが形成され、その中をライセンスが送信される。このとき、ハードディスクユニット４０において、ハードディスクユニット４１の正当性の確認がハードディスクユニット４１の証明書の認証処理によって行なわれる。このような、２つのハードディスクユニット間でライセンスの送信を行なう場合に、ライセンスの送信元であるハードディスクユニット４０側の処理を「複製／移動」と称することとする。また、複製／移動においては、ライセンスが複製されるか移動されるかはライセンスの内に記載される制御情報に従う。このとき、ライセンスの受信先のハードディスクユニット４１側の処理は、図１におけるハードディスクユニット４０の処理と同じ「書込」であり、端末装置２０とハードディスクユニット４０は、図１で示したコンテンツ提供装置３０と見ることができる。詳細については後述する。

【００３６】図３においては、１つの端末装置２０に対して２つのハードディスクユニット４０，４１が接続されている構成のみを示したが、ハードディスクユニット４１が他の端末装置に装着され、他の端末装置が端末装置２０と通信ケーブルなどで接続され、端末装置間でデータ通信が可能であれば同様な処理を行なうことも可能である。

【００３７】このような構成において、コンテンツデータの著作権を保護し、ユーザが自由にコンテンツデータを再生して楽しむためにシステム上必要とされるのは、第１には、コンテンツデータを暗号化する方式そのものであり、第２には、ライセンスの通信時におけるライセンスの漏洩を防ぐための方式であり、第３には、コンテンツデータの無断コピーによる利用を防止するためにコンテンツデータの利用方法や複製を制限する著作権保護機能である。

【００３８】本発明の実施の形態においては、特に、配信、複製／移動および使用許諾の各処理の発生時において、これらのライセンスの出力先に対する認証およびチェック機能を充実させ、非認証のハードディスクユニットおよび端末装置に対するコンテンツデータの出力を防止することによってコンテンツ鍵の流出を防ぎ、著作権の保護を強化する構成を説明する。

【００３９】なお、以下の説明においては、ダウンロードサーバ１０から、端末装置２０に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

【００４０】図４は、本発明において使用されるデータ、ライセンスの特性を説明する図である。

【００４１】まず、ダウンロードサーバ１０より配信されるデータについて説明する。Ｄｃは、映像データ等のコンテンツデータである。コンテンツデータＤｃは、コンテンツ鍵Ｋｃで復号可能な暗号化が施される。コンテンツ鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）がこの形式でダウンロードサーバ１０から端末装置２０のユーザに配布される。

【００４２】なお、以下においては、Ｅ（Ｘ，Ｙ）という表記は、データＹを暗号鍵Ｘにより暗号化したことを示すものとする。

【００４３】さらに、ダウンロードサーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する平文情報としての付加情報Ｄｉが配布される。なお、付加情報Ｄｉは、コンテンツデータＤｃを識別するためのデータＩＤ（ＤＩＤ）を含む。

【００４４】また、ライセンスとしては、コンテンツ鍵Ｋｃ、ライセンスＩＤ（ＬＩＤ）、データＩＤ（ＤＩＤ）、および制御情報ＡＣ等が存在する。

【００４５】データＩＤは、コンテンツデータＤｃを識別するためのコードであり、ライセンスＩＤは、ダウンロードサーバ１０からのライセンスの配信を管理し、個々のライセンスを識別するためのコードである。制御情報ＡＣは、ハードディスクユニットからのライセンスまたはコンテンツ鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報などがある。

【００４６】以後、ライセンスＩＤと、データＩＤと、コンテンツ鍵Ｋｃと、制御情報ＡＣとを併せて、ライセンスＬＩＣと総称することとする。

【００４７】また、以降では、簡単化のため制御情報ＡＣは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）と、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）との２項目とする。

【００４８】図５は、本発明においてセキュアコネクション形成のために利用されるデータ、鍵の特性を説明するための図である。

【００４９】端末装置２０内の再生回路１５５０、およびハードディスクユニット４０，４１には固有の公開暗号鍵ＫＰｃｘｙが設けられる。ここで、公開暗号鍵ＫＰｃｘｙは、機器のクラス（種類などの一定の単位）ごとに付与され、ｘは、再生回路とハードディスクユニットとを識別する識別子である。機器が再生回路等の再生装置である場合ｘ＝ｐであり、機器がハードディスクユニットである場合ｘ＝ｍとする。また、ｙは、機器のクラスを識別する識別子である。公開暗号鍵ＫＰｃｘｙは、秘密復号鍵Ｋｃｘｙによって復号可能である。これら公開暗号鍵ＫＰｃｘｙおよび秘密復号鍵Ｋｃｘｙは、再生回路およびハードディスクユニットの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵が共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００５０】また、ハードディスクユニットおよび再生回路の証明書としてＣｘｙが設けられる。これらの証明書は、再生回路、およびハードディスクユニットのクラスごとに異なる情報を有する。

【００５１】再生回路およびハードディスクユニットの証明書Ｃｘｙは、ＫＰｃｘｙ／／ｌｃｘｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））の形式で出荷時に再生回路およびハードディスクユニットに記録される。なお、ｌｃｘｙは、クラスごとにまとめられた機器およびクラス公開暗号鍵ＫＰｃｘｙに関する情報データである。また、Ｈ（Ｘ）は、データ列Ｘに対するＨａｓｈ関数による演算結果であるＸのハッシュ値を意味し、Ｘ／／ＹはＸとＹとの連結を意味する。Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））は、ＫＰｃｘｙ／／ｌｃｘｙの署名データである。

【００５２】ＫＰａはデータ配信システム全体で共通の公開認証鍵であり、クラス公開暗号鍵ＫＰｃｘｙとクラス情報ｌｃｘｙとを認証局においてマスタ鍵Ｋａで暗号化された署名データを復号する。マスタ鍵Ｋａは、認証局において証明書内の署名データを作成するために使用される秘密暗号鍵である。

【００５３】また、ハードディスクユニット４０，４１内のデータ処理を管理するための鍵として、ハードディスクユニット４０，４１ごとに設定される公開暗号鍵ＫＰｏｍｚと、公開暗号鍵ＫＰｏｍｚで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｏｍｚとが存在する。これらのハードディスクユニットごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｏｍｚを個別公開暗号鍵、秘密復号鍵Ｋｏｍｚを個別秘密復号鍵と称する。ｚはハードディスクユニットを識別する個々の識別子である。

【００５４】ライセンスの配信、移動、複製および使用許諾が行なわれるごとにダウンロードサーバ１０、端末装置２０、およびハードディスクユニット４０，４１において生成される共通鍵Ｋｓ１ｗ，Ｋｓ２ｗが用いられる。

【００５５】ここで、共通鍵Ｋｓ１ｗ，Ｋｓ２ｗは、ダウンロードサーバ、再生回路もしくはハードディスクユニット間の通信において、セキュアコネクションを形成する通信あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。以下においては、これらの共通鍵Ｋｓ１ｗ，Ｋｓ２ｗを「セッション鍵」とも呼ぶこととする。また、ｗは、セッションを識別するための識別子である。

【００５６】セッション鍵Ｋｓ１ｗは、ライセンスを出力する提供元あるいは送信元において発生され、セッション鍵Ｋｓ２ｗは、ライセンスを受取る提供先あるいは受信先において発生される。具体的には、ダウンロードサーバに代表されるライセンス提供装置ではＫｓ１ｗが、再生回路ではＫｓ２ｗが、そして、ハードディスクユニットでは、「書込」においてはＫｓ２ｗ、「移動／複製」においてはｋｓ１ｗが発生される。各処理において発生したセッション鍵を交換する。機器は、他の機器において発生したセッション鍵によるデータの復号処理を行なう機能を備える。このようにセッション鍵を用いてセキュアコネクションを構築し、ライセンスの送信をセキュアコネクションを介して行なうことによって、ライセンスに関する処理のセキュリティ強度を向上させ、通信に対する攻撃からライセンスを保護することができる。

【００５７】図６は、図１に示したダウンロードサーバ１０の構成を示す概略ブロック図である。

【００５８】ダウンロードサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやデータＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機等の端末装置の各ユーザごとにコンテンツデータへのアクセスの開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリアとデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００５９】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５によって制

御され、配信処理時にセッション鍵Ｋｓ１ｗを発生するためのセッション鍵発生部３１６と、ハードディスクユニットから送られてきた認証のための認証データＣｘｙ＝ＫＰｃｘｙ／／ｌｃｘｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））を復号するための公開復号鍵である認証鍵ＫＰａを保持する認証鍵保持部３１３と、ハードディスクユニットから送られてきた認証のための認証データＣｘｙを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッション鍵発生部３１６により生成されたセッション鍵Ｋｓ１ｗを復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｃｘｙを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッション鍵Ｋｓ１ｗによって暗号化された上で送信されたデータをバスＢＳ１より受けて、セッション鍵Ｋｓ１ｗにより復号処理を行なう復号処理部３２０とを含む。

【００６０】データ処理部３１０は、さらに、配信制御部３１５から与えられるコンテンツ鍵Ｋｃおよび制御情報ＡＣを、復号処理部３２０によって得られたハードディスクユニットの個別公開暗号鍵ＫＰｏｍｚによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッション鍵Ｋｓ２ｗによってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００６１】ダウンロードサーバ１０の配信処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【００６２】図７は、図１および図２に示したダウンロードサーバ１０への接続機能と再生回路１５５０を備える端末装置２０の構成を説明するための概略ブロック図である。

【００６３】ダウンロードサーバ１０とデジタル通信網とを介して接続し、データの送受信を行なう送受信部１１０４と、端末装置２０の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して端末装置２０の動作を制御するためのコントローラ１１０６と、外部からの指示を端末装置２０に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００６４】端末装置２０は、さらに、ダウンロードサーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なハードディスクユニット４０と、ハードディスクユニット４０とバスＢＳ２との間のデータの授受を制御するためのハードディスクインタフェース１２００と再生回路１５５０とを含む。

【００６５】再生回路１５５０は、証明書Ｃｐ３＝ＫＰｃｐ３Ｚ／／ｌｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））を保持する証明書保持部１５００を含む。ここで、端末装置２０のクラスｙは、ｙ＝３であるとする。

【００６６】端末装置２０は、さらに、クラス固有の復号鍵であるＫｃｐ３を保持するＫｃｐ保持部１５０２と、バスＢＳ２から受けたデータを復号鍵Ｋｃｐ３によって復号し、ハードディスクユニット４０によって発生されたセッション鍵Ｋｓ１ｗを得る復号処理部１５０４とを含む。

【００６７】端末装置２０は、さらに、ハードディスクユニット４０に記憶されたコンテンツデータを復号するライセンスの使用許諾を受ける使用許諾処理においてハードディスクユニット４０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッション鍵Ｋｓ２ｗを乱数等により発生するセッション鍵発生部１５０８と、ライセンスの使用許諾においてハードディスクユニット４０からコンテンツ鍵Ｋｃおよび再生制御情報を受取る際に、セッション鍵発生部１５０８により発生されたセッション鍵Ｋｓ２ｗを復号処理部１５０４によって得られたハードディスクユニット４０で生成されたセッション鍵Ｋｓ１ｗによって暗号化し、バスＢＳ２に出力する暗号処理部１５０６とを含む。

【００６８】端末装置２０は、さらに、バスＢＳ２上のデータをセッション鍵Ｋｓ２ｗによって復号して、コンテンツ鍵Ｋｃを出力する復号処理部１５１０と、バスＢＳ２より暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を受けて、復号処理部１５１０からのコンテンツ鍵Ｋｃによって暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号してコンテンツデータＤｃをコンテンツデコーダ１５１８へ出力する復号処理部１５１６とを含む。

【００６９】端末装置２０は、さらに、復号処理部１５１６からの出力を受けてコンテンツデータＤｃを再生するためのコンテンツデコーダ１５１８と、再生された映像信号を外部へ出力する端子１５３０とを含む。

【００７０】また、ハードディスクインタフェース１２００は、ＡＴＡ（ＡＴ　Ａｔａｃｈｍｅｎｔ）規格に準じたインタフェースであるとする。したがって、データバスＢＳは、ＡＴＡバスである。

【００７１】端末装置２０の各構成部分の各処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【００７２】図８は、図１に示すハードディスクユニット４０の構成を説明するための概略ブロック図である。ハードディスクユニット４０は、円盤状磁気記録媒体であるハードディスク１４３０，１４３１と、ヘッド１４３２～１４３４と、支柱１４３５と、アーム１４３５Ａ～１４３５Ｃと、モータ１４３６と、サーボ制御部１４３７と、シーク制御部１４３８と、記憶読出処理部１４３９と、記憶素子１４４０と、コントローラ１４４１と、コマンドセレクタ１４４２と、ＡＴＡ（ＡＴＡＴｔ

ａｃｈｍｅｎｔ）インタフェース１４４３と、端子１４４４とを含む。

【００７３】ハードディスク１４３０，１４３１は、ダウンロードサーバ１０または他のハードディスクユニットから受信した暗号化コンテンツデータを記憶するための媒体である。ヘッド１４３２は、アーム１４３５Ａの先端に固定されており、ハードディスク１４３０の一方面にデータを記憶および／または読出を行なう。また、ヘッド１４３３は、アーム１４３５Ｂの先端に固定されており、ハードディスク１４３０の他方面とハードディスク１４３１の一方面とにデータを記憶および／または読出を行なう。さらに、ヘッド１４３４は、アーム１４３５Ｃの先端に固定されており、ハードディスク１４３１の他方面にデータを記憶および／または読出を行なう。アーム１４３５Ａ～１４３５Ｃは、支柱１４３５に固定されている。

【００７４】モータ１４３６は、所定の回転数でハードディスク１４３０，１４３１を回転する。サーボ制御部１４３７は、コントローラ１４４１からの制御により所定の回転数で回転するようにモータ１４３６を制御する。シーク制御部１４３８は、コントローラ１４４１からの制御によりアーム１４３５Ａ～１４３５Ｃをハードディスク１４３０，１４３１の径方向にシークする。記憶読出処理部１４３９は、コントローラ１４４１からの制御により暗号化コンテンツデータをアーム１４３５Ａ～１４３５Ｃに固定されたヘッド１４３２～１４３４を介してハードディスク１４３０，１４３１に記憶および／または読出を行なう。

【００７５】コントローラ１４４１は、コマンドセレクタ１４４２から暗号化コンテンツデータを受け、その受けた暗号化コンテンツデータをハードディスク１４３０，１４３１の所定の場所に記憶および／または読出を行なうようにサーボ制御部１４３７、シーク制御部１４３８および記憶読出処理部１４３９を制御する。コマンドセレクタ１４４３は、ＡＴＡインタフェース１４４３から暗号かコンテンツデータおよびライセンスを受け、その受けた暗号化コンテンツデータをコントローラ１４４１へ出力し、ライセンスを記憶素子１４４０へ出力する。ＡＴＡインタフェース１４４３は、端子１４４４とコマンドセレクタ１４４２との間でデータのやり取りを行なう。端子１４４４は、端末装置２０のハードディスクインタフェース１２００との間でデータをやり取りするための端子である。

【００７６】既に説明したように、ハードディスクユニット４０のクラス公開暗号鍵およびクラス秘密復号鍵としてＫＰｃｍｙおよびＫｃｍｙがそれぞれ設けられ、ハードディスクユニットのクラス証明書Ｃｍｙ＝ＫＰｃｍｙ／／ｌｃｍｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／ｌｃｍｙ））が設けられるが、ハードディスクユニット４０においては、クラス識別子ｙ＝１で表わされるものとする。また、ハードディスクユニットを識別する個別識別子ｚはｚ＝２で表されるものとする。そして、これらは、ライセンスを直接管理する記憶素子１４４０内で管理されている。

【００７７】したがって、記憶素子１４４０は、認証データＣｍ１＝ＫＰｃｍ１／／ｌｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１））を保持する証明書保持部１４００と、ハードディスクユニットごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｏｍ２を保持するＫｏｍ保持部１４０２と、クラス秘密復号鍵Ｋｃｍ１を保持するＫｃｍ保持部１４２１と、個別秘密復号鍵Ｋｏｍ２によって復号可能な公開暗号鍵ＫＰｏｍ２を保持するＫＰｏｍ保持部１４１６とを含む。

【００７８】このように、ハードディスクユニットという記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をハードディスクユニット単位で実行することが可能になる。

【００７９】記憶素子１４４０は、さらに、コマンドセレクタ１４４２と内部バスインタフェース１４２４との間でデータのやり取りを行なう端子１４２３と、端子１４２３との間でデータを授受する内部バスインタフェース１４２４と、内部バスインタフェース１４２４との間で信号をやり取りするバスＢＳ３と、バスＢＳ３に内部バスインタフェース１４２４から与えられるデータを、Ｋｃｍ保持部１４２１からのクラス秘密復号鍵Ｋｃｍ１により復号して、書込処理においてハードディスクユニット４０の外部（ライセンスの送信元）において生成されたセッション鍵Ｋｓ１ｗを暗号処理部１４１６に出力する復号処理部１４２２と、ＫＰａ保持部１４１４から認証鍵ＫＰａを受けて、バスＢＳ３に与えられるデータから認証鍵ＫＰａによる他の機器（再生回路、または他のハードディスクユニット）の証明書の正当性を判断する認証処理を行ない、認証結果をコントローラ１４２０に、得られたクラス公開暗号鍵を暗号処理部１４１０に出力する認証処理部１４０８と、復号処理部１４２２から出力されたダウンロードサーバ１０が発生したセッション鍵Ｋｓ１ｗまたは復号処理部１４１２から出力される再生回路１５５０が発生したセッション鍵Ｋｓ２ｗによって、データを暗号化してバスＢＳ３に出力する暗号処理部１４０６とを含む。

【００８０】記憶素子１４４０は、さらに、書込処理においてセッション鍵Ｋｓ１ｗを、移動／複製および使用許諾の各処理においてセッション鍵Ｋｓ２ｗを発生するセッション鍵発生部１４１８と、セッション鍵発生部１４１８が出力したセッション鍵Ｋｓ１ｗ，Ｋｓ２ｗを認証処理部１４０８によって得られるクラス公開暗号鍵ＫＰｃｐｚもしくはＫＰｃｍｚによって暗号化してバスＢＳ３によりセッション鍵発生部１４１８にて生成したＫｓ１ｗまたはＫｓ２ｗによって暗号化コンテンツデータ

を送出する暗号処理部１４１０と、バスＢＳ３よりセッション鍵Ｋｓ２ｗによって暗号化されたデータを受けてセッション鍵発生部１４１８より得たセッション鍵Ｋｓ２ｗによって復号する復号処理部１４１２と、ライセンスの使用許諾処理においてセキュアデータ記憶領域１４１５から読出されたコンテンツ鍵Ｋｃを、移動／複製処理において復号処理部１４１２で復号された他のハードディスクユニットの個別公開暗号鍵ＫＰｏｍｚ（ｚ≠２）で暗号化する暗号処理部１４１７とを含む。

【００８１】記憶素子１４４０は、さらに、バスＢＳ３上のデータを個別公開暗号鍵ＫＰｏｍ２と対をなすハードディスクユニット４０の個別秘密復号鍵Ｋｏｍ２によって復号するための復号処理部１４０４と、ライセンスを記憶するセキュアデータ記憶領域１４１５と、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ３との間で制御情報ＡＣを受けて、記憶素子１４４０の動作を制御するためのコントローラ１４２０を含む。

【００８２】なお、ライセンスを記憶するセキュアデータ記憶領域１４１５は、ハードディスクユニット４０において、ハードディスク１４３０，１４３１に障害が発生してデータの読出をできない状態になった場合であっても、ライセンスの読出を保証するために、つまり、移動／複製処理が提供できるように、ハードディスク１４３０，１４３１に対する記憶／読出とは独立してアクセス可能であり、かつ、ハードディスクユニット１４３０，１４３１より安定な記録媒体である半導体メモリによって構成される。また、記憶素子１４４０は、セキュリティ確保の観点から、耐タンパ構造を備えた１つの半導体素子によって構成される。

【００８３】なお、記憶素子１４４０は、ハードディスクユニット４０に着脱可能な半導体素子として構成することも可能である。

【００８４】ここでは、記憶素日１４４０は、１つの半導体素子として構成しているが、複数の半導体素子によって構成することも可能である。このような場合に、記憶素子を構成する複数の半導体素子間の配線が観測されることでライセンスが漏洩することがないように、当該半導体素子間の配線を隠さなければならない。

【００８５】このように、記憶素子１４４０を設けることで、ライセンスに関する機密性と安全性を確保することができる。

【００８６】ハードディスクユニット４０は、２枚のハードディスク１４３０，１４３１を含むが、ハードディスク１４３０，１４３１にデータを記録および／または再生するとき、ハードディスク１４３０にデータを記録および／または再生した後にハードディスク１４３１にデータを記録および／または再生するように１枚づつ、データが記録および／または再生されるのではなく、複数のヘッド１４３２～１４３４が同時に同じ位置へ移動し、その移動した位置に同時にデータを記録および／または再生する。したがって、２枚のハードディスク１４３０，１４３１の全体で１つのデータ記憶領域を構成する。

【００８７】図９は、ハードディスク１４３０，１４３１の全体で構成されるデータ記憶領域の構成図を示したものである。図９を参照して、データ記憶領域２０００は、ユーザ領域２１００と、非ユーザ領域２２００とを含む。ユーザ領域２１００は、データ記憶領域２１１０から成る。非ユーザ領域２２００は、管理データ記憶領域２２１０から成る。

【００８８】データ領域２０００は、データ領域内の記録単位ごとの記録位置を指定する実アドレス０～Ｍ＋Ｎが設けられている。ユーザ領域には、データ領域の実アドレス０～Ｍによって指定されるＭ＋１個の領域が割当てられ、管理データ領域には、データ領域の実アドレスＮ＋１～Ｎ＋Ｍで指定されるＭ個の領域が割当てられる。１つのデータ領域は５１２バイトのデータが記録可能である。

【００８９】ユーザ領域２１００には、インタフェース１４４３を介してデータの記憶および／または読出が直接行なえる領域であり、記録位置の指定には、ＬＢＡと呼ばれる論理アドレスが用いられる。従って、ユーザ領域には２つのアドレスが存在し、外部からはＬＢＡによって指示し、内部では実アドレスに変換して、記憶および／または読出を行なう構成となっている。このように構成することで、指定された記録位置に不良が発生し、使用不可能となっても、その不良位置を指定していたＬＢＡに対して、不良が発生した記録位置の割当てを破棄し、予め準備しておいた代替領域を割当てることでＬＢＡにおける連続性を保証する。また、ユーザ領域へのインタフェース１４４３を介したデータの記憶および／または読出は、標準ＡＴＡコマンド（ライト／リード命令）によってＬＢＡを指定することで実行される。

【００９０】図９においては、ＬＢＡは実アドレスに一致しているが、必ずしも、一致するものではないが、必ず、１つのＬＢＡに対して１つの実アドレスが存在する。

【００９１】管理データ領域２２１０は、先に説明した代替のための予備の領域とハードディスクユニット４０内にて独自に使用される管理データが記憶される領域である。管理データが記憶される領域には、ハードディスク１４３０，１４３１に記憶したデータ記録に関する管理データ（データ領域の代替情報、エラーログ、実アドレスとＬＢＡマッピングテーブルなど）や、コントローラ１４４１のプログラムの一部などが記録されている。管理データ領域２２１０は、インタフェース１４４３を介してデータの記憶および／または読出を行なうことはできない。ただし、代替処理によってＬＢＡが割当てられた記録位置は、ユーザ領域２１００の一部として利用される。

17

【００９２】また、記憶素子１４４０内のセキュアデータ記憶領域１４１５の記録位置の指定方法として以下においては、セキュアデータ記憶領域１４１５は、ｎ個の記録領域に対して割当てられた記録位置を示すエントリ番号によって行なうものとする。それぞれに付与されたエントリ番号を指定することでライセンスの書込、移動／複製および使用許諾処理を行なうことが可能である。記憶素子１４４０はへのアクセスについては、ユーザ領域２１００と異なる複数の拡張ＡＴＡコマンドを一定の順序で指示することで、通信先との間にセキュアコネクションを構築し、構築後、エントリ番号を指示することでライセンスの記憶／読出を行なうものとする。コマンドセレクタ１４４２は、ＡＴＡコマンドを確認し、標準ＡＴＡコマンドであれば、コントローラ１４４１へ、拡張ＡＴＡコマンドであれば記憶素子１４４０の端子１４２３、内部バスＩＦ１４２４、バスＢＳ３を介してコントローラ１４２０へ伝える。

【００９３】セキュアデータ記憶領域１４１５の記録位置の指定方法として、ユーザ領域２１００の論理アドレスであるＬＢＡとは、独立したエントリ番号を用いるとして説明したが、ハードディスクユニット４０の記録領域を一元管理する意味で、セキュアデータ記憶領域１４１５の記録位置の指定方法をデータ領域２１００に割当てられたＬＢＡと連続するＬＢＡを割当てて管理してもよい。この場合、たとえば、エントリ番号０～ｎが論理アドレスＬＢＡのｍａｘＬＢＡ＋１～ｍａｘＬＢＡ＋ｎ＋１に割当てることができる。

【００９４】ハードディスクユニット４１については、その構成はハードディスクユニット同一であるため説明を省略する。また、ハードディスクユニット４１のクラス識別子ｙは、ハードディスクユニット４０と同一のｙ＝１とし、個別識別子ｚは、ｚ＝４（≠２）とであるとする。

【００９５】データ記憶領域２１１０は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）、付加情報Ｄｉ、暗号化コンテンツデータの再生リストおよびライセンスを管理するためのライセンス管理ファイルを記憶する。管理データ記憶領域２２１０は、データ記憶領域２１１０にデータを記憶および／または読出を行なうために必要な管理情報を記憶する。

【００９６】以下、図１、図２および図３におけるライセンスに関する処理について詳細に説明する。

【００９７】［配信処理］図１に示すダウンロードサーバ１０からハードディスクユニット４０への暗号化コンテンツデータを復号するライセンスの配信について説明する。図１０および図１１は、図１に示すダウンロードサーバ１０からライセンスを配信する動作を説明するための第１および第２のフローチャートである。ハードディスクユニット４０は、書込処理を行なっている。

【００９８】図１０における処理以前に、端末装置２０

18

のユーザは、ダウンロードサーバ１０に対して電話網を介して接続し、ダウンロードを希望するコンテンツに対するデータＩＤを取得し、ダウンロードサーバ１０に対して配信要求を行なっていること、さらに、ハードディスクユニット４０のセキュアデータ記憶領域１４１５の記憶状況を把握して、セキュアデータ記憶領域１４１５の空き領域を確認して、新たにライセンスを記録するセキュアデータ記憶領域１４１５上の記憶位置を指定する格納先のエントリ番号を決定していることを前提としている。また、本フローチャートに従ったハードディスクユニット４０へのデータの入出力および支持は、拡張ＡＴＡコマンドを用いて行なわれる。

【００９９】図１０を参照して、端末装置２０のユーザから操作パネル１１０８を介してライセンスの配信処理が指示される。

【０１００】ライセンスの配信処理が指示されると、コントローラ１１０６は、バスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０へ証明書の出力要求を出力する（ステップＳ１００）。ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４、およびＡＴＡインタフェース１４４３を介して証明書の出力要求を受理し、その受理した証明書の出力要求を記憶素子１４４０の端子１４２３へ出力し、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して証明書の出力要求を受理する（ステップＳ１０２）。そして、コントローラ１４２０は、バスＢＳ３を介して証明書保持部１４００から証明書Ｃｍ１を読出し、証明書Ｃｍ１をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介して出力し、コマンドセレクタ１４４２は、証明書Ｃｍ１をＡＴＡインタフェース１４４３および端子１４４４を介してハードディスクインタフェース１２００へ出力する（ステップＳ１０４）。

【０１０１】端末装置２０のコントローラ１１０６は、ハードディスクユニット４０からの証明書Ｃｍ１をハードディスクインタフェース１２００およびバスＢＳ２を介して受理し（ステップＳ１０６）、その受理した証明書Ｃｍ１およびライセンス購入条件のデータＡＣをダウンロードサーバ１０に対して送信し（ステップＳ１０８）、ダウンロードサーバ１０は、端末装置２０から認証データＣｍ１、およびライセンス購入条件のデータＡＣを受理する（ステップＳ１１０）。そして、復号処理部３１２は、ハードディスクユニット４０から出力された証明書Ｃｍ１＝ＫＰｃｍ１／／ｌｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１））の署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を認証鍵保持部３１３からの認証鍵ＫＰａで復号し、その復号したデータであるハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を配信制御部３１５へ出力する。配信制御部３１５は、証明

書Ｃｍ１のＫＰｃｍ１／／ｌｃｍ１に対するハッシュ値を演算し、その演算したハッシュ値が復号処理部３１２から受けたハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）に一致するか否かを確認する。すなわち、ダウンロードサーバ１０は、復号処理部３１２が証明書Ｃｍ１の署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を認証鍵ＫＰａで復号できること、および配信制御部３１５が送信元であるハードディスクユニット４０から受信したハッシュ値と自ら演算したハッシュ値とが一致することを確認することにより証明書Ｃｍ１を検証する（ステップＳ１１２）。

【０１０２】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した証明書を受信したか否かを判断する認証処理を行なう。正当な証明書であると判断した場合、配信制御部３１５は、次の処理（ステップＳ１１４）へ移行する。正当な証明書でない場合には、非承認とし、エラー通知を端末装置２０へ出力し（ステップＳ１７６）、端末装置２０はエラー通知を受理し（ステップＳ１７８）、書込拒否により配信動作が終了する（ステップＳ１８０）。

【０１０３】認証の結果、正当な証明書を持つハードディスクユニットを装着した端末装置からのアクセスであることが確認されると、ダウンロードサーバ１０において、配信制御部３１５は、ハードディスクユニット４０からのクラス公開暗号鍵ＫＰｃｍ１を受理し（ステップＳ１１４）、配信要求のあったライセンスを識別するためのライセンスＩＤを生成する（ステップＳ１１６）。

【０１０４】その後、配信制御部３１５は、端末装置２０から受理したライセンスの購入条件に基づいて、制御情報ＡＣを生成し（ステップＳ１１８）、セッション鍵発生部３１６は、配信のためのセッション鍵Ｋｓ１ａを生成する（ステップＳ１２０）。セッション鍵Ｋｓ１ａは、復号処理部３１２によって得られたハードディスクユニット４０に対応するクラス公開暗号鍵ＫＰｃｍ１によって、暗号処理部３１８によって暗号化される（ステップＳ１２２）。

【０１０５】配信制御部３１５は、ライセンスＩＤおよび暗号化されたセッション鍵Ｋｓ１ａを、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）として、バスＢＳ１および通信装置３５０を介して端末装置２０へ送信する（ステップＳ１２４）。

【０１０６】端末装置２０がデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受信すると（ステップＳ１２６）、コントローラ１１０６は、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）をバスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０へ出力し（ステップＳ１２８）、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受け、その受けたデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を端子１４２３へ出力する。そうすると、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ１３０）。そして、コントローラ１４２０は、バスＢＳ３を介して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｃｍ保持部１４２１に保持されるハードディスクユニット４０に固有なクラス秘密復号鍵Ｋｃｍ１によって復号処理を行なうことにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ１３２）。

【０１０７】そうすると、ダウンロードサーバ１０の配信制御部３１５は、セッション鍵の出力要求をバスＢＳ１および通信装置３５０を介して端末装置２０へ送信し、端末装置２０のコントローラ１１０６は、セッション鍵の出力要求を受信してハードディスクインタフェース１２００を介してハードディスクユニット４０へ送信する（ステップＳ１３４）。ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してセッション鍵の出力要求を受け、その受けたセッション鍵の出力要求を記憶素子１４４０の端子１４２３へ出力する。そして、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してセッション鍵の出力要求を受理し、セッション鍵を発生するようにセッション鍵発生部１４１８を制御する。そして、セッション鍵発生部１４１８は、セッション鍵Ｋｓ２ａを生成する（ステップＳ１３６）。

【０１０８】そうすると、暗号処理部１４０６は、復号処理部１４２２より切換スイッチ１４２５の接点Ｐａを介して与えられるセッション鍵Ｋｓ１ａによって、セッション鍵発生部１４１８から切換スイッチ１４２６の接点Ｐｄを介して与えられるセッション鍵Ｋｓ２ａ、およびＫＰｏｍ保持部１４１６から切換スイッチ１４２６の接点Ｐｆを介して与えられる個別公開暗号鍵ＫＰｏｍ２を１つのデータ列として暗号化して、暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３に出力する（ステップＳ１３８）。コントローラ１４２０は、バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）にライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０に出力する（ステップＳ１４

０）。

【０１０９】そして、端末装置２０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）を受理し（ステップＳ１４２）、その受理したデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をダウンロードサーバ１０に送信する（ステップＳ１４４）。

【０１１０】ダウンロードサーバ１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）を受信し（ステップＳ１４６）、復号処理部３２０は、暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をセッション鍵Ｋｓ１ａによって復号し、ハードディスクユニット４０で生成されたセッション鍵Ｋｓ２ａ、およびハードディスクユニット４０の個別公開暗号鍵ＫＰｏｍ２を受理する（ステップＳ１４８）。

【０１１１】そして、配信制御部３１５は、データＩＤ（ＤＩＤ）およびコンテンツ鍵Ｋｃを情報データベース３０４から取得してライセンスＬＩＣを生成する（ステップＳ１５０）。その後、配信制御部３１５は、生成したライセンスＬＩＣ、すなわち、ライセンスＩＤ、データＩＤ、コンテンツ鍵Ｋｃ、および制御情報ＡＣを暗号処理部３２６に与え、暗号処理部３２６は、復号処理部３２０によって得られたハードディスクユニット４０の個別公開暗号鍵ＫＰｏｍ２によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を生成する（ステップＳ１５２）。

【０１１２】図１１を参照して、暗号処理部３２８は、暗号処理部３２６からの暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を、復号処理部３２０により復号されたセッション鍵Ｋｓ２ａによってさらに暗号化して暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を生成する（ステップＳ１５４）。そして、配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を端末装置２０へ出力し（ステップＳ１５６）、端末装置２０は、暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を受理する（ステップＳ１５８）。

【０１１３】そして、端末装置２０のコントローラ１１０６は、暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））をバスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０へ出力し（ステップＳ１６０）、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を受け、その受けた暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を記憶素子１４４０の端子１４２３へ出力する。記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））を受理する（ステップＳ１６２）。コントローラ１４２０は、受理した暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））をバスＢＳ３を介して復号処理部１４１２に与え、復号処理部１４１２は、暗号化データＥ（Ｋｓ２ａ，（ＫＰｏｍ２，ＬＩＣ））をセッション鍵発生部１４１８からのセッション鍵Ｋｓ２ａによって復号し、暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を受理する（ステップＳ１６４）。

【０１１４】そうすると、復号処理部１４０４は、復号処理部１４１２からの暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）をＫｏｍ保持部１４０２からの個別秘密復号鍵Ｋｏｍ２によって復号し、ライセンスＬＩＣを受理する（ステップＳ１６６）。コントローラ１４２０がライセンスＬＩＣを受理すると、端末装置２０のコントローラ１１０６は、ライセンスＬＩＣを格納するためのエントリをバスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０へ出力し（ステップＳ１６８）、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してエントリ番号を受け、その受けたエントリ番号を記憶素子１４４０の端子１４２３へ出力する。

【０１１５】そうすると、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してエントリ番号を受理する（ステップＳ１７０）。そして、コントローラ１４２０は、既に受理したライセンスＩＤと、ステップＳ１６６において受理したライセンスＬＩＣに含まれるライセンスＩＤとが一致するか否かを判定し（ステップＳ１７２）、両者が不一致であるときエラー通知をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力する。そして、コマンドセレクタ１４４２は、エラー通知をＡＴＡインタフェース１４４３および端子１４４４を介してハードディスクインタフェース１２００へ出力し（ステップＳ１７４）、端末装置２０のコントローラ１１０６は、エラー通知をハードディスクインタフェース１２００およびバスＢＳ２を介して受理し（ステップＳ１７８）、書込拒否によって配信動作が終了する（ステップＳ１８０）。

【０１１６】一方、ステップＳ１７２において、２つのライセンスＩＤが一致すると判定されたとき、コントローラ１４２０は、セキュアデータ記憶領域１４１５のうち、ステップＳ１７０において受理したエントリ番号によって指定される領域にライセンスＬＩＣを記録し（ステップＳ１８２）、一連の動作が正常に終了する（ステップＳ１８４）。

【０１１７】なお、上記においては説明しなかったが、ライセンスの配信処理が終了した後、端末装置２０のコントローラ１１０６は、暗号化コンテンツデータの配信要求をダウンロードサーバ１０へ送信し、ダウンロード

サーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、ダウンロードサーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して端末装置２０へ送信する。

【０１１８】端末装置２０は、データＥ（Ｋｃ，Ｄｃ）／／Ｄｉを受信して、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを受理する。そうすると、コントローラ１１０６は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを１つのコンテンツファイルとしてバスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０に入力する。また、コントローラ１１０６は、ハードディスクユニット４０に格納されたライセンスのエントリと、平文のライセンスＩＤと、データＩＤとを含み、かつ、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）と付加情報Ｄｉとに対するライセンス管理ファイルを生成し、その生成したライセンス管理ファイルをバスＢＳ２およびハードディスクインタフェース１２００を介してハードディスクユニット４０に入力する。そして、ハードディスクユニット４０において、コマンドセレクタ１４４２は、受理した暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）、付加情報Ｄｉ、およびライセンス管理ファイルをコントローラ１４４１へ出力する。そして、コントローラ１４４１は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）、付加情報Ｄｉ、およびライセンス管理ファイルをヘッド１４３２～１４３４を介してハードディスク１４３０，１４３１のデータ記憶領域２１１０に記録するように記憶読出処理部１４３９を制御し、記憶読出処理部１４３９は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）、付加情報Ｄｉ、およびライセンス管理ファイルをハードディスク１４３０，１４３１に記録する。

【０１１９】さらに、端末装置２０のコントローラ１１０６は、ハードディスクユニット４０のデータ記憶領域２１１０に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報Ｄｉから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

【０１２０】このようにして、端末装置２０に装着されたライセンスを記憶するハードディスクユニット４０が正規の証明書を保持する機器であること、同時に、公開暗号鍵ＫＰｃｍ１が有効であることを確認した上でライセンスを配信することができ、不正なハードディスクユニットへのライセンスの配信を禁止することができる。

【０１２１】また、ダウンロードサーバおよびハードディスクユニットでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１２２】図１２は、ハードディスクユニット４０のデータ記憶領域２０００およびセキュアデータ記憶領域１４１５を示したものである。データ記憶領域２１１０には、再生コンテンツリストファイル１６０と、コンテンツファイル１６１１～１６１ｋと、ライセンス管理ファイル１６２１～１６２ｋとが記憶されている。コンテンツファイル１６１１～１６１ｋは、受信した暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）と付加情報Ｄｉとを１つのファイルとして記憶する。また、ライセンス管理ファイル１６２１～１６２ｋは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記憶されており、セキュアデータ記憶領域１４１５に記憶したライセンスＬＩＣのエントリを格納する。

【０１２３】ハードディスクユニット４０は、ダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、または他のハードディスクユニットから暗号化コンテンツデータおよびライセンスを複製／移動処理によって受信したとき、暗号化コンテンツデータをハードディスク１４３０，１４３１に記憶し、ライセンスをセキュアデータ記憶領域１４１５に記憶する。

【０１２４】ハードディスクユニット４０に送信された暗号化コンテンツデータのライセンスはセキュアデータ記憶領域１４１５のエントリによって指定された領域に記憶され、ハードディスク１４３０，１４３１のデータ記憶領域２１１０に記憶された再生コンテンツリストファイル１６０のライセンス管理ファイルを読出せば、ライセンスが格納されるセキュアデータ記憶領域１４１５上のエントリ番号を取得でき、その取得したエントリによって対応するライセンスをセキュアデータ記憶領域１４１５から読出すことができる。

【０１２５】また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記憶されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、端末装置２０が他の端末装置から暗号化コンテンツデータだけを受信した場合や、ライセンスだけを他のハードディスクユニットに移動させた場合に相当する。

【０１２６】さらに、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、端末装置２０がダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の端末装置へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

【０１２７】［ハードディスクユニット間移動／複製処

理］上述したように、ハードディスクユニット４０のデータ記憶領域２１１０に記憶されている暗号化コンテンツデータは、データ記憶領域２１１０に記憶されたデータが標準ＡＴＡコマンドによって記憶および／または読出できることから、図３に示す構成において、ハードディスクユニット４０に記憶された暗号化コンテンツデータは、ハードディスクユニット４１に自由に複製することができる。しかし、暗号化コンテンツデータを他のハードディスクユニット４１に複製しても、その複製したコンテンツデータを復号するためのライセンスを取得しなければ複製した暗号化コンテンツデータを再生することができない。

【０１２８】このように、図１に示す構成において、端末装置２０にハードディスクユニット４０に代えてハードディスクユニット４１を装着したライセンスの配信を図１０および図１１のフローチャートに従って受けることも可能であるが、図３に示す構成においてハードディスクユニット４０に記憶されているライセンスを、ハードディスクユニット４１に移動あるいは複製することができる。上述したように、ハードディスクユニット４０における処理が移動／複製処理であり、ハードディスクユニット４１における処理が書込処理である。

【０１２９】図１３および図１４は、図３におけるハードディスクユニット４０に記録されたライセンスをハードディスクユニット４１に移動／複製するための第１および第２のフローチャートである。なお、図１２における処理以前に、端末装置２０，２１のコントローラ１１０６は、ユーザがライセンスの移動／複製を行なうコンテンツの指定およびライセンスの移動／複製リクエストを行なうための入力手段（図示せず）に接続され、ユーザによってなされたライセンスの移動／複製を行なうコンテンツの指定、およびライセンスの移動／複製リクエストを受取る。そして、コントローラ１１０６は、送信元であるハードディスクユニット４０内のコンテンツリストファイル１６０を参照して、移動または複製を行なうライセンスのコンテンツ管理ファイルを特定し、その特定したコンテンツ管理ファイルを参照して移動または複製するライセンスが記憶されているハードディスクユニット４０のセキュアデータ記憶部１４１５内のエントリ番号を取得していること、および受信先のハードディスクユニット４１のセキュアデータ記憶部１４１５内の空き領域を確認し、移動または複製されたライセンスを記憶するためのエントリ番号を決定していることを前提にしている。

【０１３０】図１３を参照して、移動／複製リクエストがユーザから指示されると、端末装置２１のコントローラ１１０６は、証明書の出力要求をバスＢＳを介してハードディスクユニット４１へ送信する（ステップＳ２００）。そして、ハードディスクユニット４１のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して証明書の出力要求を受け、その受けた証明書の出力要求を記憶素子１４４０の端子１４２３へ出力する。

【０１３１】そうすると、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して証明書の出力要求を受信する（ステップＳ２０２）。そして、コントローラ１４２０は、証明書の出力要求を受信すると、証明書保持部１４００から証明書Ｃｍ１をバスＢＳ３を介して読出し、その読出した証明書Ｃｍ１をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、証明書Ｃｍ１をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２１のコントローラ１１０６へ出力する（ステップＳ２０４）。そして、コントローラ１１０６は、バスＢＳを介して証明書Ｃｍ１を受理し（ステップＳ２０６）、バスＢＳを介してハードディスクユニット４０へハードディスクユニット４１の証明書Ｃｍ１を送信する（ステップＳ２０８）。

【０１３２】そうすると、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して証明書Ｃｍ１を受理し（ステップＳ２１０）、コマンドセレクタ１４４２は、証明書Ｃｍ１を記憶素子１４４０の端子１４２３へ出力する。記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して証明書Ｃｍ１を受け、その受けた証明書Ｃｍ１をバスＢＳ３を介して認証処理部１４０８へ与える。そして、認証処理部１４０８は、ＫＰａ保持部１４１４からの認証鍵ＫＰａによって証明書Ｃｍ１の復号処理を実行し、その復号結果をコントローラ１４２０へ出力する。コントローラ１４２０は、証明書Ｃｍ１のデータＫＰｃｍ１／／ｌｃｍ１に対するハッシュ値を演算し、その演算したハッシュ値が認証処理部１４０８から受けたハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）に一致するか否かを確認する。すなわち、ハードディスクユニット４０は、認証処理部１４０８が証明書Ｃｍ１の暗号化データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１））を認証鍵ＫＰａで復号できること、およびコントローラ１４２０が送信元であるハードディスクユニット４１から受信したハッシュ値と自ら演算したハッシュ値とが一致することを確認することにより証明書Ｃｍ１を検証する（ステップＳ２１２）。

【０１３３】正当な証明書であると判断した場合、コントローラ１４２０は、次の処理（ステップＳ２１４）へ移行する。正当な証明書でない場合には、非承認とし、エラー通知を端末装置２０を介して端末装置２１へ出力し（ステップＳ２８２）、端末装置２１はエラー通知を受理し（ステップＳ２８４）、書込拒否により移動／複

製動作が終了する（ステップＳ２８６）。

【０１３４】認証の結果、正当な証明書を持つハードディスクユニットを装着した端末装置からのアクセスであることが確認されると、ハードディスクユニット４０において、コントローラ１４２０は、ハードディスクユニット４１からのクラス公開暗号鍵ＫＰｃｍ１を受理し（ステップＳ２１４）、セッション鍵Ｋｓ１ｂを生成するようにセッション鍵発生部１４１８を制御し、セッション鍵発生部１４１８はセッション鍵Ｋｓ１ｂを生成する（ステップＳ２１６）。

【０１３５】その後、セッション鍵Ｋｓ１ｂは、認証処理部１４０８によって得られたハードディスクユニット４１に対応するクラス公開暗号鍵ＫＰｃｍ１によって、暗号処理部１４１０によって暗号化される（ステップＳ２１８）。

【０１３６】コントローラ１４２０は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ３を介して暗号処理部１４１０から受け、その受けた暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０，２１へ送信する（ステップＳ２２０）。

【０１３７】端末装置２０，２１が暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を受信すると（ステップＳ２２２）、コントローラ１１０６は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）に移動／複製の対象となるライセンスを識別するライセンスＩＤを加えたデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳを介してハードディスクユニット４１へ出力し（ステップＳ２２４）、ハードディスクユニット４１のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理する（ステップＳ２２６）。そして、コマンドセレクタ１４４２は、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を記憶素子１４４０の端子１４２３へ出力し、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理する。コントローラ１４２０は、バスＢＳ３を介して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｃｍ保持部１４２１に保持されるハードディスクユニット４１に固有なクラス秘密復号鍵Ｋｃｍ１によって復号処理を行なうことにより、セッション鍵Ｋｓ１ｂを復号し、セッション鍵Ｋｓ１ｂを受理する（ステップＳ２２８）。

【０１３８】そうすると、端末装置２１のコントローラ１１０６は、セッション鍵の出力要求をバスＢＳを介してハードディスクユニット４１へ出力し（ステップＳ２３０）、ハードディスクユニット４１のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してセッション鍵の出力要求を受ける。そして、コマンドセレクタ１４４２は、セッション鍵の出力要求を記憶素子１４４０の端子１４２３へ出力し、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してセッション鍵の出力要求を受理し、セッション鍵を発生するようにセッション鍵発生部１４１８を制御する。

【０１３９】セッション鍵発生部１４１８は、コントローラ１４２０の制御に応じてセッション鍵Ｋｓ２ｂを生成し（ステップＳ２３２）、暗号処理部１４０６は、復号処理部１４２２より与えられるセッション鍵Ｋｓ１ｂによって、セッション鍵発生部１４１８から切換スイッチ１４２６の接点Ｐｄを介して与えられるセッション鍵Ｋｓ２ｂ、およびＫＰｏｍ保持部１４１６から切換スイッチ１４２６の接点Ｐｆを介して与えられる個別公開暗号鍵ＫＰｏｍ４を１つのデータ列として暗号化して、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）をバスＢＳ３に出力する（ステップＳ２３４）。コントローラ１４２０は、バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）にライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力する。そして、コマンドセレクタ１４４２は、データＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０，２１に出力し（ステップＳ２３６）、端末装置２０，２１は、バスＢＳを介してデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）を受理し（ステップＳ２３８）、その受理したデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）をハードディスクユニット４０へ出力する（ステップＳ２４０）。

【０１４０】ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）を受信し（ステップＳ２４２）、その受信したデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）を記憶素子１４４０の端子１４２３へ出力する。そして、記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）を受け、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）を復号処理部１４１２に与える。

【０１４１】そうすると、復号処理部１４１２は、暗号

29

化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ４）をセッション鍵Ｋｓ１ｂによって復号し、ハードディスクユニット４１で生成されたセッション鍵Ｋｓ２ｂ、およびハードディスクユニット４１の個別公開暗号鍵ＫＰｏｍ４を受理する（ステップＳ２４４）。

【０１４２】そして、端末装置２０のコントローラ１１０６から移動／複製の対象となるライセンスＬＩＣの記憶されているエントリ番号が出力され（ステップＳ２４６）、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してエントリ番号を受け、その受けたエントリ番号を記憶素子１４４０の端子１４２３へ出力する。記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してライセンスＬＩＣの記憶されているエントリ番号を受理する（ステップＳ２４８）。そして、コントローラ１４２０は、受理したエントリ番号に基づいて、セキュアデータ記憶領域１４１５から移動または複製の対象となるライセンスＬＩＣを取得する（ステップＳ２５０）。コントローラ１４２０は、取得したライセンスＬＩＣの有効フラグが有効か否かを判定する（ステップＳ２５２）。有効フラグが有効でないと判定されたとき、上述したようにコントローラ１４２０はエラー通知を出力し、書込拒否により移動／複製動作が終了する（ステップＳ２８２，Ｓ２８４，Ｓ２８６）。

【０１４３】ステップＳ２５２において、有効フラグが有効であると判定されると、コントローラ１４２０は、取得したライセンスＬＩＣを暗号処理部１４１７に与え、暗号処理部１４１７は、復号処理部１４１２からの個別公開暗号鍵ＫＰｏｍ４によってライセンスＬＩＣを暗号化し、暗号化データＥ（ＫＰｏｍ４，ＬＩＣ）を生成する（ステップＳ２５４）。

【０１４４】図１４を参照して、コントローラ１４２０は、ステップＳ２５０において取得したライセンスＬＩＣに含まれる制御情報ＡＣに基づいてライセンスをハードディスクユニット４１へ複製／移動することが禁止されていないか否かを確認する（ステップＳ２５６）。そして、複製／移動が禁止されているときステップＳ２８２，Ｓ２８４を経て書込拒否によって移動／複製の動作が終了する（ステップＳ２８６）。ライセンスの複製が許可されているときステップＳ２６０へ移行する。一方、ライセンスの移動が許可されているときコントローラ１４２０は、取得した有効フラグを無効に変更する（ステップＳ２５８）。

【０１４５】そして、ステップＳ２５６において複製が許可されていると判定されたとき、またはステップＳ２５８の後、暗号処理部１４０６は、暗号処理部１４１７からの暗号化データＥ（ＫＰｏｍ４，ＬＩＣ）を、復号処理部１４１２により復号されたセッション鍵Ｋｓ２ｂによってさらに暗号化して暗号化データＥ（Ｋｓ２ｂ，

30

（ＫＰｏｍ４，ＬＩＣ））を生成する（ステップＳ２６０）。そして、コントローラ１４２０は、バスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介して暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））をコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０，２１へ出力する（ステップＳ２６２）。

【０１４６】そうすると、端末装置２０，２１は、暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））を受理し（ステップＳ２６４）、端末装置２１のコントローラ１１０６は、暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））をバスＢＳ介してハードディスクユニット４１へ出力する（ステップＳ２６６）。そして、ハードディスクユニット４１のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））を受け、その受けた暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））を記憶素子１４４０の端子１４２３へ出力する。

【０１４７】記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））を受理する（ステップＳ２６８）。コントローラ１４２０は、受理した暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））をバスＢＳ３を介して復号処理部１４１２に与え、復号処理部１４１２は、暗号化データＥ（Ｋｓ２ｂ，（ＫＰｏｍ４，ＬＩＣ））をセッション鍵発生部１４１８からのセッション鍵Ｋｓ２ｂによって復号し、暗号化データＥ（ＫＰｏｍ４，ＬＩＣ）を受理する（ステップＳ２７０）。

【０１４８】復号処理部１４０４は、復号処理部１４１２から暗号化データＥ（ＫＰｏｍ４，ＬＩＣ）を受け、その受けた暗号化データＥ（ＫＰｏｍ４，ＬＩＣ）をＫｏｍ保持部１４０２からの個別秘密復号鍵Ｋｏｍ４によって復号し、ライセンスＬＩＣを受理する（ステップＳ２７２）。

【０１４９】端末装置２１のコントローラ１１０６は、ライセンスＬＩＣのエントリ番号をバスＢＳを介してハードディスクユニット４１へ出力し（ステップＳ２７４）、ハードディスクユニット４１のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してエントリ番号を受け、その受けたエントリ番号を記憶素子１４４０の端子１４２３へ出力する。記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介してライセンスＬＩＣの格納先であるエントリ番号を受理する（ステップＳ２７６）。

【０１５０】そして、コントローラ１４２０は、ライセ

ンスＬＩＣに含まれるライセンスＩＤが既に受理しているライセンスＩＤに一致するか否かを判定し（ステップＳ２７８）、２つのライセンスＩＤが不一致であるときバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してエラー通知をコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、エラー通知をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０，２１へ出力する（ステップＳ２８０）。そして、端末装置２０のコントローラ１１０６は、エラー通知を受理し（ステップＳ２８４）、書込拒否によって移動／複製処理が終了する（ステップＳ２８６）。

【０１５１】一方、ステップＳ２７８において、２つのライセンスＩＤが一致すると判定されたとき、コントローラ１４２０は、セキュアデータ記憶領域１４１５のうち受理したエントリ番号によって指定された領域にライセンスＬＩＣを記録し（ステップＳ２８８）、ライセンスの移動／複製動作が正常に終了する（ステップＳ２９０）。

【０１５２】なお、暗号化コンテンツデータのハードディスクユニット４０からハードディスクユニット４１への移動／複製は、ライセンスの移動／複製が終了した後、ハードディスクユニット４０のデータ記憶領域２１１０から暗号化コンテンツデータを読出してハードディスクユニット４１へ送信することによって行なえばよい。

【０１５３】また、受信側のハードディスクユニット４１に対しては、移動／複製したライセンスに対するライセンス管理ファイルが既に記録されている場合には、ライセンス管理ファイルに対して格納位置などの書込みを行なうことで対象のライセンス管理ファイルを更新する。また、対象となるライセンス管理ファイルがハードディスクユニット４１に記録されていない場合には、新たにライセンス管理ファイルを生成し、その生成したライセンス管理ファイルを受信側のハードディスクユニット４１に記録する。

【０１５４】このようにして、端末装置２１に装着されたハードディスクユニット４１が正規の機器であること、同時に、クラス公開暗号鍵ＫＰｃｍ１が有効であることを確認した上で、正規なハードディスクユニットへの移動要求に対してのみライセンスを移動することができ、不正なハードディスクユニットへの移動を禁止することができる。

【０１５５】また、ハードディスクユニットで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動／複製の動作におけるセキュリティを向上させることができる。

【０１５６】［使用許諾処理］上述したように、端末装置２０に装着されたハードディスクユニット４０は、ダウンロードサーバ１０から、直接、暗号化コンテンツデータおよびライセンスを受信できる。ハードディスクユニット４０に対して、ダウンロードサーバ１０から、直接、暗号化コンテンツデータを受信し、記録する処理について説明した。また、ハードディスクユニット４１に対して、ハードディスクユニット４０から暗号化コンテンツデータを複製によって、ライセンスを「移動／複製」という概念によって受信し、記憶する処理について説明した。

【０１５７】そこで、次に、これらの各種の方法によってハードディスクユニットが受信したライセンスの使用許諾について説明する。ライセンスを保持するのは、ハードディスクユニットであり、暗号化コンテンツデータを再生するのは、端末装置２０の再生回路１５５０である。そして、再生回路１５５０は、暗号化コンテンツデータを再生するとき自己が正規の機器であることをハードディスクユニット４０に対して証明した後、ハードディスクユニット４０からライセンスを受信する。したがって、この動作は、ハードディスクユニット４０にとっては、端末装置２０の再生回路１５５０に対してライセンスの使用を許諾することに相当する。

【０１５８】そこで、再生回路１５５０におけるライセンスを用いた暗号化コンテンツデータの再生処理を再生回路１５５０へのライセンスの使用許諾処理と考えることにする。

【０１５９】図２を参照して、コントローラ１１０６と再生回路１５５０とを内蔵した端末装置２０はバスＢＳを介してハードディスクユニット４０とデータのやり取りを行ない、再生回路１５５０はハードディスクユニット４０からライセンスの使用許諾を受ける。したがって、ライセンスの使用許諾の説明は図２に示す概念図を用いて行なう。

【０１６０】図１５は、ハードディスクユニット４０から端末装置２０の再生回路１５５０に対する、暗号化コンテンツデータを復号するライセンスの使用許諾処理を説明するためのフローチャートである。ハードディスクユニット４１を端末装置２０に装着してもライセンスの使用許諾は可能であり、この場合も図１５に示すフローチャートに従ってライセンスの使用許諾が行なわれる。

【０１６１】なお、図１５における処理以前に、端末装置２０のユーザは、ハードディスクユニット４０のデータ記憶領域２１１０に記憶されている再生リストに従って、再生するコンテンツを決定し、コンテンツファイルとライセンス管理ファイルを特定し、ライセンス管理ファイルからライセンスの格納されているエントリ番号を取得していることを前提として説明する。

【０１６２】図１５を参照して、使用許諾動作の開始とともに、端末装置２０のユーザから操作パネル１１０８

を介して使用許諾リクエストが端末装置２０にインプットされる。そうすると、コントローラ１１０６は、バスＢＳ２を介して証明書の出力要求を出力し（ステップＳ３００）、再生回路１５５０は、証明書の出力要求を受理する（ステップＳ３０２）。そして、再生回路１５５０は、証明書Ｃｐ３をコントローラ１１０６へ出力し（ステップＳ３０４）、コントローラ１１０６は、証明書Ｃｐ３を受理し（ステップＳ３０６）、バスＢＳを介してハードディスクユニット４０へ証明書Ｃｐ３を出力する（ステップＳ３０８）。

【０１６３】そうすると、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して証明書Ｃｐ３を受け、その受けた証明書Ｃｐ３を記憶素子１４４０の端子１４２３へ出力する。記憶素子１４４０のコントローラ１４２０は、端子１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して証明書Ｃｐ３＝ＫＰｃｐ３／／ｌｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））を受理し（ステップＳ３１０）、認証処理部１４０８は、受理した証明書Ｃｐ３のうち、署名データＥ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））をＫＰａ保持部１４１４に保持された認証鍵ＫＰａによって復号し、その復号したハッシュ値Ｈ（ＫＰｃｐ３／／ｌｃｐ３）をコントローラ１４２０へ出力する。コントローラ１４２０は、証明書Ｃｐ３のうちデータＫＰｃｐ３／／ｌｃｐ３に対するハッシュ値を演算し、その演算したハッシュ値が再生回路１５５０において演算されたハッシュ値Ｈ（ＫＰｃｐ３／／ｌｃｐ３）に一致するか否かを確認する。そして、コントローラ１４２０は、再生回路１５５０から受理した証明書Ｃｐ３のうち、署名データＥ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））が認証処理部１４０８において復号されたこと、および２つのハッシュ値が一致することを確認することにより再生回路１５５０から受理した証明書Ｃｐ３を検証する（ステップＳ３１２）。証明書Ｃｐ３が非承認である場合、コントローラ１４２０は、バスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へエラー通知を出力し、コマンドセレクタ１４４２は、ＡＴＡインタフェース１４４３および端子１４４４を介してエラー通知を端末装置２０のコントローラ１１０６へ出力し（ステップＳ３７０）、コントローラ１１０６は、エラー通知を受理する（ステップＳ３７２）。そして、使用拒否によって一連の動作が終了する（ステップＳ３７４）。

【０１６４】証明書が承認された場合、コントローラ１４２０は、再生回路１５５０からのクラス公開暗号鍵ＫＰｃｐ３を受理し（ステップＳ３１４）、セッション鍵Ｋｓ１ｄを生成するようにセッション鍵発生部１４１８を制御し、セッション鍵発生部１４１８はセッション鍵Ｋｓ１ｄを生成する（ステップＳ３１６）。

【０１６５】その後、セッション鍵Ｋｓ１ｄは、認証処理部１４０８によって得られた再生回路１５５０に対応するクラス公開暗号鍵ＫＰｃｐ３によって、暗号処理部１４１０によって暗号化される（ステップＳ３１８）。

【０１６６】コントローラ１４２０は、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をバスＢＳ３を介して暗号処理部１４１０から受け、その受けた暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をバスＢＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０へ送信する（ステップＳ３２０）。

【０１６７】端末装置２０が暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受信すると（ステップＳ３２２）、コントローラ１１０６は、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をバスＢＳ２を介して再生回路１５５０へ出力し（ステップＳ３２４）、再生回路１５５０は、バスＢＳ２を介して、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受理する（ステップＳ３２６）。そして、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）は復号処理部１５０４に与えられ、復号処理部１５０４は、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をＫｃｐ保持部１５０２からのクラス秘密復号鍵Ｋｃｐ３によって復号し、ハードディスクユニット４０において生成されたセッション鍵Ｋｓ１ｄを受理する（ステップＳ３２８）。

【０１６８】そうすると、セッション鍵発生部１５０８は、使用許諾用のセッション鍵Ｋｓ２ｄを生成し（ステップＳ３３０）、その生成したセッション鍵Ｋｓ２ｄを暗号処理部１５０６へ出力する。暗号処理部１５０６は、セッション鍵発生部１５０８からのセッション鍵Ｋｓ２ｄを復号処理部１５０４からのセッション鍵Ｋｓ１ｄによって暗号化して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を生成し（ステップＳ３３２）、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）をコントローラ１１０６へ出力する（ステップＳ３３４）。そして、コントローラ１１０６は、バスＢＳ２を介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受理し（ステップＳ３３６）、バスＢＳを介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）をハードディスクユニット４０へ出力する（ステップＳ３３８）。

【０１６９】そうすると、ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受け、その受けた暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を記憶素子１４４０の端子１４２３へ出力する。そして、記憶素子１４４０の復号処理部１４１２は、端子１４２３、内部バスインタフェース１４２４、およびバスＢＳ３を介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受ける（ステップＳ３４

０）。復号処理部１４１２は、セッション鍵発生部１４１８において発生されたセッション鍵Ｋｓ１ｄによって暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を復号して、再生回路１５５０で生成されたセッション鍵Ｋｓ２ｄを受理する（ステップＳ３４２）。

【０１７０】端末装置２０のコントローラ１１０６は、バスＢＳを介してハードディスクユニット４０へ、事前に取得してあったエントリ番号を出力する（ステップＳ３４４）。

【０１７１】ハードディスクユニット４０のコマンドセレクタ１４４２は、端子１４４４およびＡＴＡインタフェース１４４３を介してエントリ番号を受け、その受けたエントリ番号を記憶素子１４４０の端子１４２３へ出力す記憶素子１４４０のコントローラ１４２０は、端子1.423、内部バスインタフェース１４２４およびバスＢＳ３を介してエントリ番号を受理し（ステップＳ３４６）、セキュアデータ記憶領域１４１５のうち、受理したエントリ番号によって指定された領域に格納された有効フラグに基づいてライセンスの有効性を判定する（ステップＳ３４８）。そして、ライセンスが無効であるとき、上述したように使用拒否によって一連の動作が終了する（ステップＳ３７０～Ｓ３７４）。

【０１７２】一方、ステップＳ３４８において、ライセンスが有効であると判定されたとき、コントローラ１４２０は、エントリ番号によって指定された領域からライセンスＬＩＣを取得し（ステップＳ３５０）、その取得したライセンスＬＩＣに含まれる制御情報ＡＣに基づいてライセンスを端末装置２０の再生回路１５５０へ使用許諾することが禁止されていないか否かを確認する（ステップＳ３５２）。そして、使用許諾が禁止されているときステップＳ３７０，Ｓ３７２を経て使用拒否によって使用許諾の動作が終了する（ステップＳ３７４）。ライセンスの使用許諾が無制限に許可されているときステップＳ３５６へ移行する。一方、ライセンスの使用許諾の回数が制限されているときコントローラ１４２０は制御情報ＡＣの使用許諾の回数を変更する（ステップＳ３５４）。

【０１７３】ステップＳ３５２において使用許諾が無制限に許可されているとき、またはステップＳ３５４の後、暗号処理部１４０６は、コンテンツ鍵Ｋｃを復号処理部１４１２により復号されたセッション鍵Ｋｓ２ｄによって暗号化し、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を生成する（ステップＳ３５６）。そして、コントローラ１４２０は、暗号処理部１４０６からの暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をバスＳ３、内部バスインタフェース１４２４および端子１４２３を介してコマンドセレクタ１４４２へ出力し、コマンドセレクタ１４４２は、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０のコントローラ１１０６へ出力し（ステップＳ３５８）、

コントローラ１１０６は、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を受理する（ステップＳ３６０）。そして、コントローラ１１０６は、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をバスＢＳ２を介して復号処理部１５１０に出力し（ステップＳ３６２）、復号処理部１５１０は、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を受理する（ステップＳ３６４）。

【０１７４】そうすると、復号処理部１５１０は、暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をセッション鍵発生部１５０８からのセッション鍵Ｋｓ２ｄによって復号し、コンテンツ鍵Ｋｃを受理する（ステップＳ３６６）。そして、使用許諾の処理が正常に終了する（ステップＳ３６８）。

【０１７５】なお、ライセンスＬＩＣの再生回路１５５０への使用許諾の動作が終了した後、コントローラ１１０６は、ハードディスクユニット４０に対して暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を要求する。そうすると、ハードディスクユニット４０のコントローラ１４４１は、データ記憶領域２１１０から暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を取得し、その取得した暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）をコマンドセレクタ１４４２へ出力する。そして、コマンドセレクタ１４４２は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）をＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０へ出力する。

【０１７６】端末装置２０のコントローラ１１０６は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を取得し、バスＢＳ２を介して暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を再生回路１５５０へ与える。

【０１７７】そして、再生回路１５５０の復号処理部１５１６は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号処理部１５１０から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

【０１７８】そして、復号されたコンテンツデータＤｃはコンテンツデコーダ１５１８へ出力され、コンテンツデコーダ１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部の出力装置（たとえば、テレビモニタ）へ出力される。ユーザは、出力装置を介して再生されたコンテンツを楽しむことができる。

【０１７９】上記においては、暗号化コンテンツデータを復号するためのライセンスを例にして説明したが、本発明において対象となるものは暗号化コンテンツデータを復号するためのライセンスに限らず、個人情報、およびクレジットカードの情報等の同時に２個以上存在してはいけない機密性が要求されるデータが対象となる。このようなデータについても、上述した各処理を行なうことができる。

【０１８０】この場合、機密性が要求されるデータをラ

イセンス内のコンテンツ鍵Ｋｃと入れ替えることにより容易に実現できる。

【０１８１】この発明によるハードディスクユニットは、図１６に示すハードディスクユニット４０Ａであってもよい。図１６を参照して、ハードディスクユニット４０Ａは、ハードディスクユニット４０のコマンドセレクタ１４４２を削除し、端子１４４５を追加したものであり、その他はハードディスクユニット４０と同じである。なお、記憶素子１４４０は、ハードディスクユニット４０Ａに脱着可能な半導体素子として構成することも可能である。

【０１８２】ハードディスクユニット４０Ａにおいては、ＡＴＡインタフェース１４４３は、端子１４４４とコントローラ１４４１との間でデータをやり取りする。また、端子１４４５は、記憶素子１４４０の端子１４２３との間でデータをやり取りする。

【０１８３】端子１４４４は、暗号化コンテンツデータ等の非機密データのハードディスクユニット４０Ａへの入出力を行なう端子であり、端子１４４５は、暗号化コンテンツデータを復号するためのライセンス等の機密データをハードディスクユニット４０Ａへ入出力するための端子である。したがって、端末装置２０のコントローラ１１０６は、ハードディスクインタフェース１２００を介して暗号化コンテンツデータをハードディスクユニット４０Ａの端子１４４４へ入出力し、ハードディスクインタフェース１２００を介してライセンスをハードディスクユニット４０Ａの端子１４４５へ入出力する。そして、ハードディスクユニット４０Ａにおいては、端子１４４４から入力された暗号化コンテンツデータは、ＡＴＡインタフェース１４４３を介してコントローラ１４４１へ入力され、コントローラ１４４１は、暗号化コンテンツデータをハードディスク１４３０，１４３１のデータ記憶領域２１１０の所定の位置に記憶するようにサーボ制御部１４３７、シーク制御部１４３８および記憶読出処理部１４３９を制御する。また、コントローラ１４４１は、ハードディスク１４３０，１４３１のデータ記憶領域２１１０の所定の位置から暗号化コンテンツデータを読出すようにサーボ制御部１４３７、シーク制御部１４３８および記憶読出処理部１４３９を制御し、記憶読出処理部１４３９が読出した暗号化コンテンツデータを受ける。そして、コントローラ１４４１は、記憶読出処理部１４３９から受けた暗号化コンテンツデータをＡＴＡインタフェース１４４３および端子１４４４を介して端末装置２０へ出力する。

【０１８４】一方、記憶素子１４４０のコントローラ１４２０は、端子１４４５，１４２３、内部バスインタフェース１４２４およびバスＢＳ３を介して、ライセンスの受信に関する各種の処理を行ない、受信したライセンスを最終的にセキュアデータ記憶領域１４１５に格納する。また、コントローラ１４２０は、ライセンスの使用許諾処理においては、バスＢＳ３、内部バスインタフェース１４２４および端子１４２３，１４４５を介して端末装置２０とやり取りし、セキュアデータ記憶領域１４１５に記憶されたライセンスを読出し、その読出したライセンスをバスＢＳ３、内部バスインタフェース１４２４および端子１４２３，１４４５を介して端末装置２０へ出力する。

【０１８５】したがって、ハードディスクユニット４０Ａを用いることにより、上述したライセンスおよび暗号化コンテンツデータの書込処理、ライセンスおよび暗号化コンテンツデータの移動／複製処理、ライセンスおよび暗号化コンテンツデータの使用許諾処理を、ライセンスに関する処理と暗号化コンテンツデータに関する処理とを並行しながら行なうことができる。そして、各処理は、上述した図１０、図１１、図１２、図１３、図１４および図１５に示すフローチャートに従って行なわれる。

【０１８６】このように、ハードディスクユニット４０Ａにおいては、暗号化コンテンツデータ等の非機密データのハードディスク１４３０，１４３１への入出力と、ライセンス等の機密データのセキュアデータ記憶領域１４１５への入出力とは独立に行なわれるので、より高速化が可能である。

【０１８７】上述したように、この発明によるハードディスクユニットにおいては、暗号化コンテンツデータ等の非機密データはハードディスクに記憶され、暗号化コンテンツデータを復号するためのライセンス等の機密データは機密性を有する記憶素子に記憶されるので、ハードディスクがクラッシュ等に破壊されても暗号化コンテンツデータを復号するためのライセンスをハードディスクユニットから取出すことができる。

【０１８８】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　コンテンツをハードディスクユニットへ記憶するためのシステムの概略構成図である。

【図２】　ハードディスクユニットに記憶されたコンテンツの再生処理を説明するための概略ブロック構成図である。

【図３】　ハードディスクユニットに記憶されたコンテンツのハードディスクユニット間の移動／複製処理を説明するための概略構成図である。

【図４】　図１に示すシステムにおいて扱われるデータ、情報などの特性を示す図である。

【図５】　図１に示すシステムにおいてデータ保護のために用いられるデータ、鍵などの特性を示す図である。

39

【図６】　図１に示すダウンロードサーバの構成を示す概略ブロック図である。

【図７】　図１に示す端末装置の構成を示す概略ブロック図である。

【図８】　図１に示すハードディスクユニットの構成を示すブロック図である。

【図９】　ハードディスクユニットにおける記憶領域の構成を示す図である。

【図１０】　図１に示すシステムにおけるライセンスの配信処理の動作を説明するための第１のフローチャートである。

【図１１】　図１に示すシステムにおけるライセンスの配信処理の動作を説明するための第２のフローチャートである。

【図１２】　ハードディスクユニットにおけるコンテンツ記憶方法を説明するための図である。

【図１３】　図３に示す構成においてライセンスの移動／複製処理の動作を説明するための第１のフローチャートである。

【図１４】　図３に示す構成においてライセンスの移動／複製処理の動作を説明するための第２のフローチャートである。

【図１５】　図２に示す構成においてライセンスの使用許諾処理の動作を説明するためのフローチャートである。

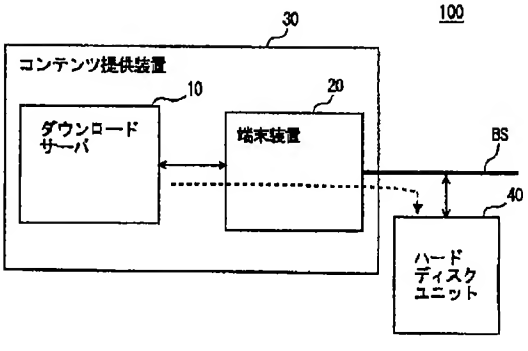
【図１６】　図１に示すハードディスクユニットの他の構成を示すブロック図である。

【符号の説明】

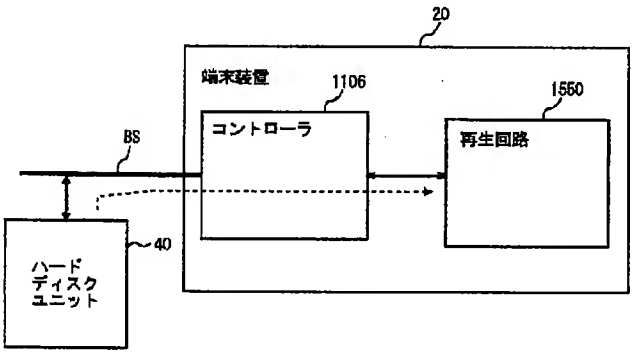
１０　ダウンロードサーバ、２０　端末装置、３０　コンテンツ提供装置、４０，４１，４０Ａ　ハードディスクユニット、１００　データ配信システム、１６０　コンテンツリストファイル、３０２　課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８，１５０８　セッション鍵発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、３５０　通信装置、１１０６，１４２０，１４４１　コントローラ、１４２３，１４４４，１４４５，１５３０　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　ハードディスクインタフェース、１４００，１５００　証明書保持部、１４０２　Ｋｏｍ保持部、１４１４　ＫＰａ保持部、１４１５　セキュアデータ記憶領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｃｍ保持部、１４３０，１４３１　ハードディスク、１４３２～１４３４　ヘッド、１４３５　支柱、１４３５Ａ～１４３５Ｃ　アーム、１４３６　モータ、１４３７　サーボ制御部、１４３８　シーク制御部、１４３９　記憶読出処理部、１４４２　コマンドセレクタ、１４４３　ＡＴＡインタフェース、１４３９　端子、１４４０　記憶素子、１４２４　内部バスインタフェース、１５０２　Ｋｃｐ保持部、１５１８　コンテンツデコーダ、１５１９　ＤＡ変換器、１５５０　再生回路、１６１１～１６１ｋ　コンテンツファイル、１６２１～１６２ｋ　ライセンス管理ファイル、２０００　データ記憶領域、２１００　ユーザ領域、２１１０　データ記憶領域、２２００　非ユーザ領域、２２１０　管理データ領域。

40

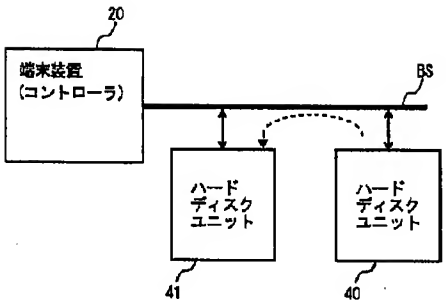
【図１】



【図２】



【図３】



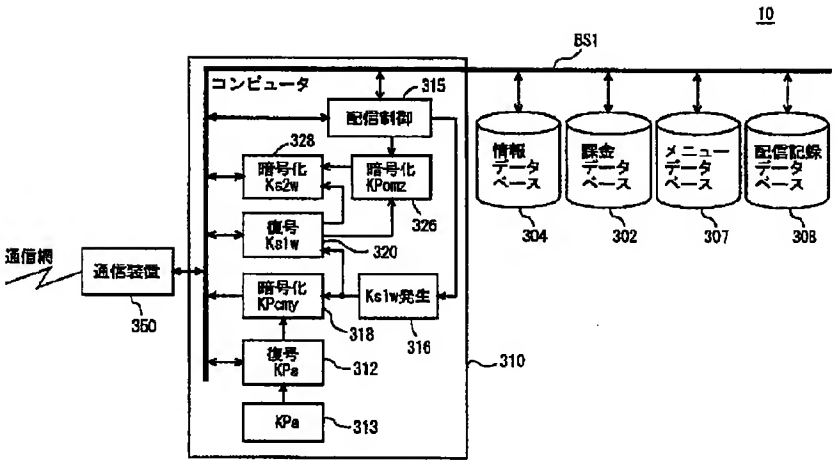
【図４】

名称	記号	属性	特性
データ	Dc	データ固有	例：映像データ、音楽データ、朗読データ、教材データ、画像データ、コンテンツ鍵にて暗号化した暗号化データE(Kc, Dc)として記録管理される
データ情報	Di	データ固有	Dcに付随する平文データ。DIDを含む
データID	DID	データ固有	データおよびコンテンツ鍵を特定するための管理コード
コンテンツ鍵	Kc	データ固有	暗号データを暗号／復号する共通鍵
制御情報	AC	ライセンス固有	再生やライセンスの取り扱いに対する制限事項
ライセンスID	LID	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	LIC	ライセンス固有	Kc//AC//DID//LIDの総称

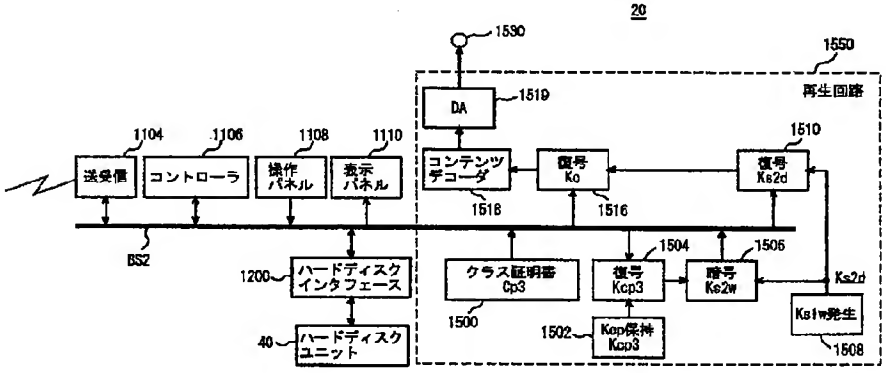
【図５】

名称	記号	特性
マスタ鍵	Ka	クラス証明書作成のために使用する秘密暗号鍵。 認証局にて運用される
認証鍵	KPa	認証局にて証明書を検証する公開復号鍵。 ライセンス提供側にて運用される
クラス公開暗号鍵	KPoxy	機器のクラス（種類などの一定の単位ごと）に付与される暗号鍵。 xは機器を識別する識別子。再生装置ではp、ハードディスクユニットではmとする。 yはクラスを識別するための識別子
クラス秘密復号鍵	Koxy	クラス公開鍵KPoxyにて暗号化されたデータを復号する非対称な復号鍵
クラス情報	Ioxy	クラスごとの機器およびクラス公開鍵に関する情報データ
クラス証明書	Cxy	KPoxy // Ioxy // E(Ka, H(KPoxy // Ioxy)) 認証鍵によってその正当性が確認できる
個別公開暗号鍵	KPomz	ハードディスクユニットごとに固有な値を持つ個別公開暗号鍵 zはハードディスクユニットを識別するための識別子
個別秘密復号鍵	Komz	個別公開鍵KPomzにて暗号化されたデータを復号する非対称な復号鍵
セッション鍵	Ks1x	ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
セッション鍵	Ks2x	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵

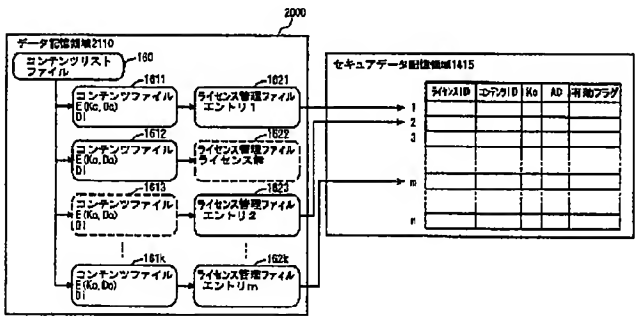
【図６】


10
BS1
コンピュータ
315
配信制御
328
暗号化 Ks2w
暗号化 KPcmz
326
復号 Ks1w
320
通信網
通信装置
350
暗号化 KPcrty
Ks1w発生
318
316
復号 KPa
312
310
KPa
313
情報データベース
304
課金データベース
302
メニューデータベース
307
配信記録データベース
308

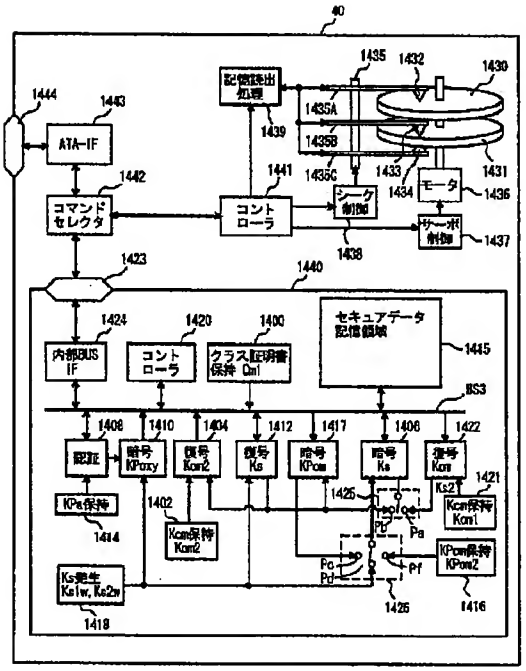
【図７】


20
1530
1550
再生回路
DA
1519
1104
1106
1108
1110
1510
送受信
コントローラ
操作パネル
表示パネル
コンテンツデコーダ
復号 Ko
復号 Ks2d
1518
1516
BS2
1504
1506
1200
ハードディスクインタフェース
クラス証明書 Cp3
復号 Kcp3
暗号 Ks2w
Ks2d
Ks1w発生
1500
1502
Kcp保持 Kcp3
1508
40
ハードディスクユニット

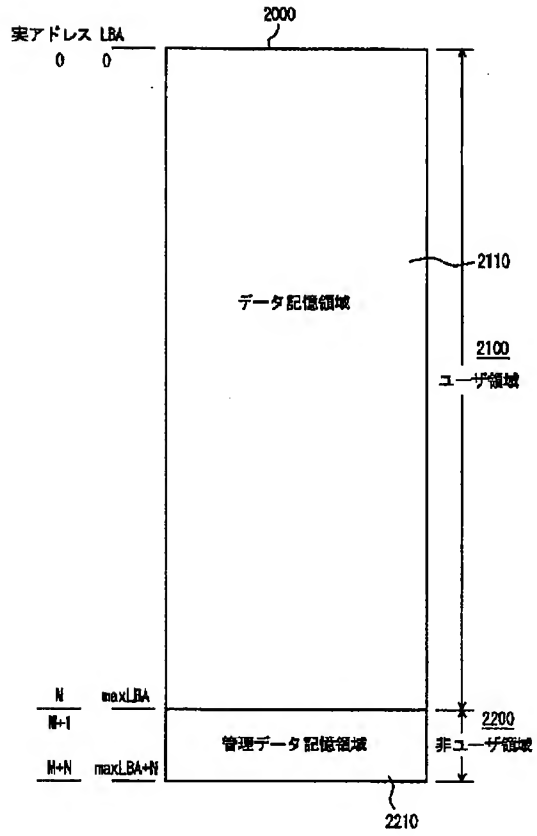
【図１２】


2000
データ記憶領域2110
コンテンツリストファイル
160
1611
コンテンツファイル E(Kc, Da) DI
ライセンス管理ファイル エントリ1
1621
1612
ライセンス管理ファイル ライセンス例
1622
1613
ライセンス管理ファイル エントリ2
1623
161k
ライセンス管理ファイル エントリm
162k
セキュアデータ記憶領域1415
ライセンスID
コンテンツID
Ko
AD
有効フラグ
1
2
3
m
n

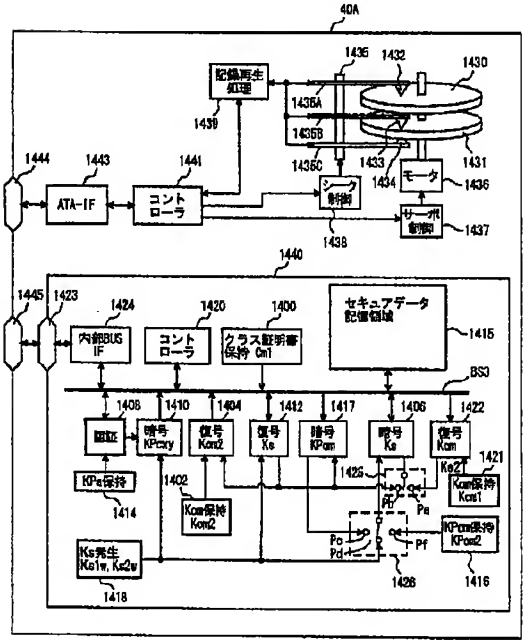
【図８】


40
1435
1432
1430
記憶読出処理
1444
1443
ATA-IF
1439
1435A
1435B
1435C
1433
1431
1441
1434
モータ
1436
1442
コマンドセレクタ
コントローラ
シーク制御
サーボ制御
1438
1437
1423
1440
セキュアデータ記憶領域
1424
1420
1400
内部BUS IF
コントローラ
クラス証明書保持 Cnt
1445
BS3
1408
1410
1404
1412
1417
1406
1422
認証
暗号 KPcxy
復号 Kcn2
復号 Ks
暗号 KPcm
暗号 Ks
暗号 Kcm
1421
Ks21
KPs保持
1425
Kcm保持 Kcm1
1402
Kcm保持 Kcm2
Pb
Pa
Pc
Pd
Pf
KPcm保持 KPcm2
Ks発生 Ks1w, Ks2w
1414
1418
1426
1416

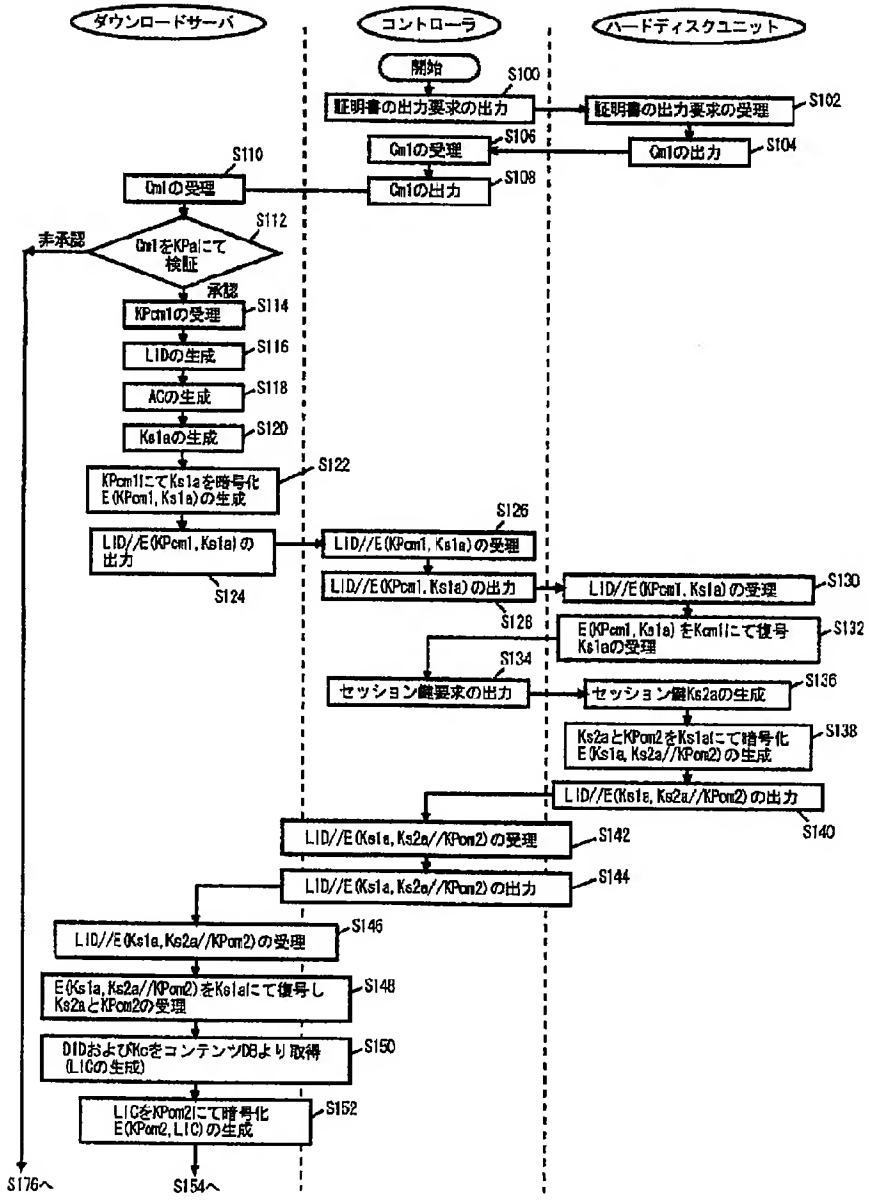
【図９】


2000
実アドレス LBA
0 0
2110
データ記憶領域
2100
ユーザ領域
N maxLBA
M+1
2200
管理データ記憶領域
非ユーザ領域
M+N maxLBA+N
2210

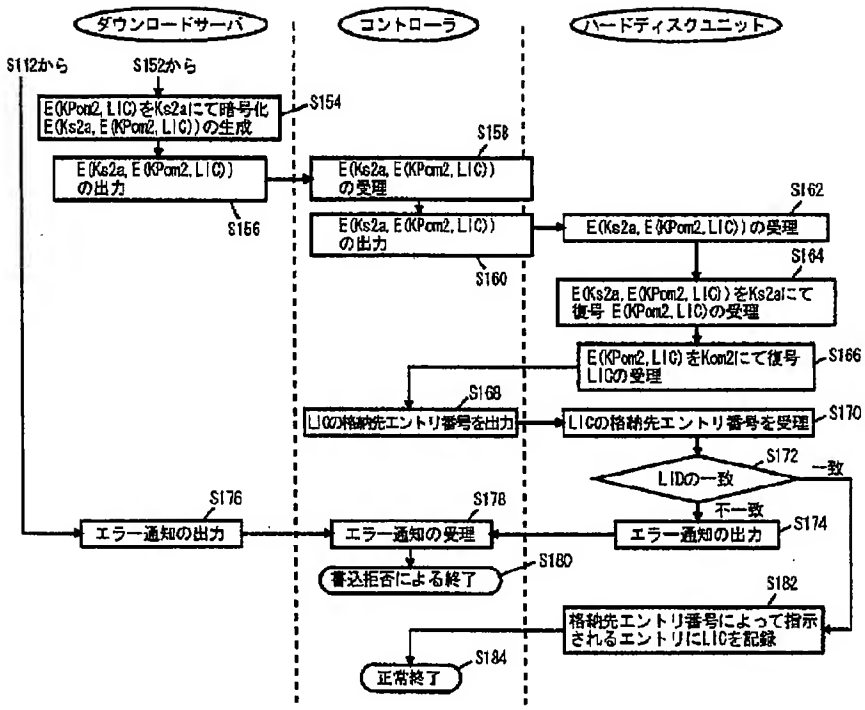
【図１６】


40A
1435
1432
1430
記憶再生処理
1439
1435A
1435B
1435C
1433
1431
1444
1443
1441
1434
モータ
1436
ATA-IF
コントローラ
シーク制御
サーボ制御
1438
1437
1440
1445
1423
1424
1420
1400
セキュアデータ記憶領域
1415
内部BUS IF
コントローラ
クラス証明書保持 Cnt
BS3
1408
1410
1404
1412
1417
1406
1422
認証
暗号 KPcxy
復号 Kcn2
復号 Ks
暗号 KPcm
暗号 Ks
復号 Kcm
1421
Ks21
KPs保持
1425
Kcm保持 Kcm1
1402
Kcm保持 Kcm2
Pb
Pa
Pc
Pd
Pf
KPcm保持 KPcm2
Ks発生 Ks1w, Ks2w
1414
1418
1426
1416

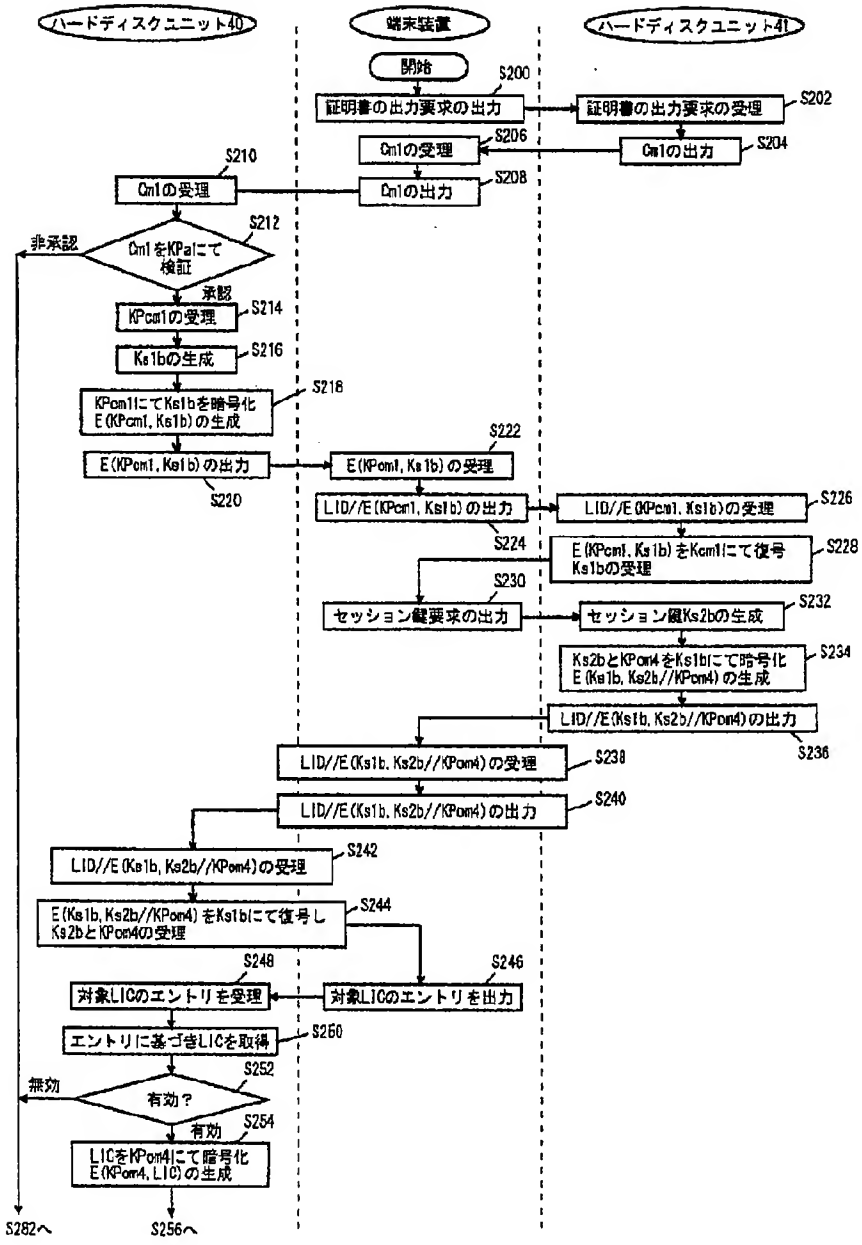
【図１０】


ダウンロードサーバ
コントローラ
ハードディスクユニット
開始
S100
証明書の出力要求の出力
S102
証明書の出力要求の受理
S106
Cm1の受理
S104
Cm1の出力
S110
Cm1の受理
S108
Cm1の出力
S112
Cm1をKPaにて検証
非承認
承認
S114
KPcm1の受理
S116
LIDの生成
S118
ACの生成
S120
Ks1aの生成
S122
KPcm1にてKs1aを暗号化 E(KPcm1, Ks1a)の生成
S126
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S124
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S130
S128
E(KPcm1, Ks1a)をKcm1にて復号 Ks1aの受理
S132
S134
セッション鍵要求の出力
セッション鍵Ks2aの生成
S136
Ks2aとKPcm2をKs1aにて暗号化 E(Ks1a, Ks2a//KPcm2)の生成
S138
LID//E(Ks1a, Ks2a//KPcm2)の出力
S140
LID//E(Ks1a, Ks2a//KPcm2)の受理
S142
LID//E(Ks1a, Ks2a//KPcm2)の出力
S144
LID//E(Ks1a, Ks2a//KPcm2)の受理
S146
E(Ks1a, Ks2a//KPcm2)をKs1aにて復号し Ks2aとKPcm2の受理
S148
DIDおよびKcをコンテンツDBより取得 (LICの生成)
S150
LICをKPcm2にて暗号化 E(KPcm2, LIC)の生成
S152
S176へ
S154へ

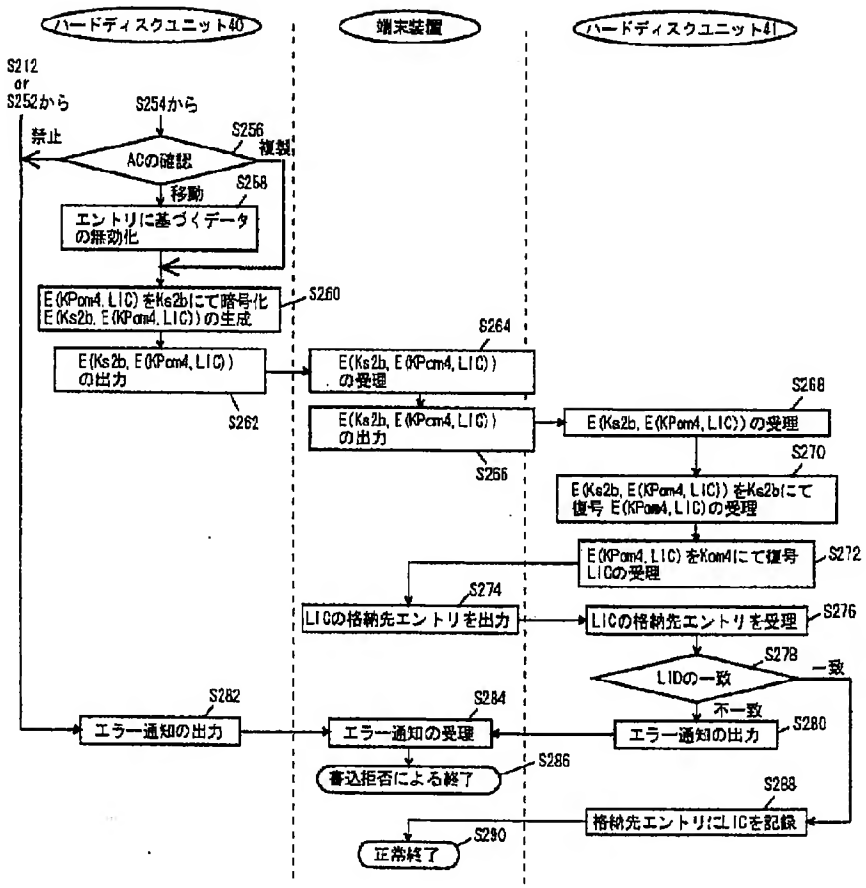
【図１１】


ダウンロードサーバ
コントローラ
ハードディスクユニット
S112から
S152から
E(KPcm2, LIC)をKs2aにて暗号化
E(Ks2a, E(KPcm2, LIC))の生成
S154
E(Ks2a, E(KPcm2, LIC))
の出力
S156
E(Ks2a, E(KPcm2, LIC))
の受理
S158
E(Ks2a, E(KPcm2, LIC))
の出力
S160
E(Ks2a, E(KPcm2, LIC))の受理
S162
E(Ks2a, E(KPcm2, LIC))をKs2aにて
復号 E(KPcm2, LIC)の受理
S164
E(KPcm2, LIC)をKcm2にて復号
LICの受理
S166
LICの格納先エントリ番号を出力
S168
LICの格納先エントリ番号を受理
S170
LIDの一致
S172
一致
不一致
エラー通知の出力
S174
エラー通知の出力
S176
エラー通知の受理
S178
書込拒否による終了
S180
格納先エントリ番号によって指示
されるエントリにLICを記録
S182
正常終了
S184

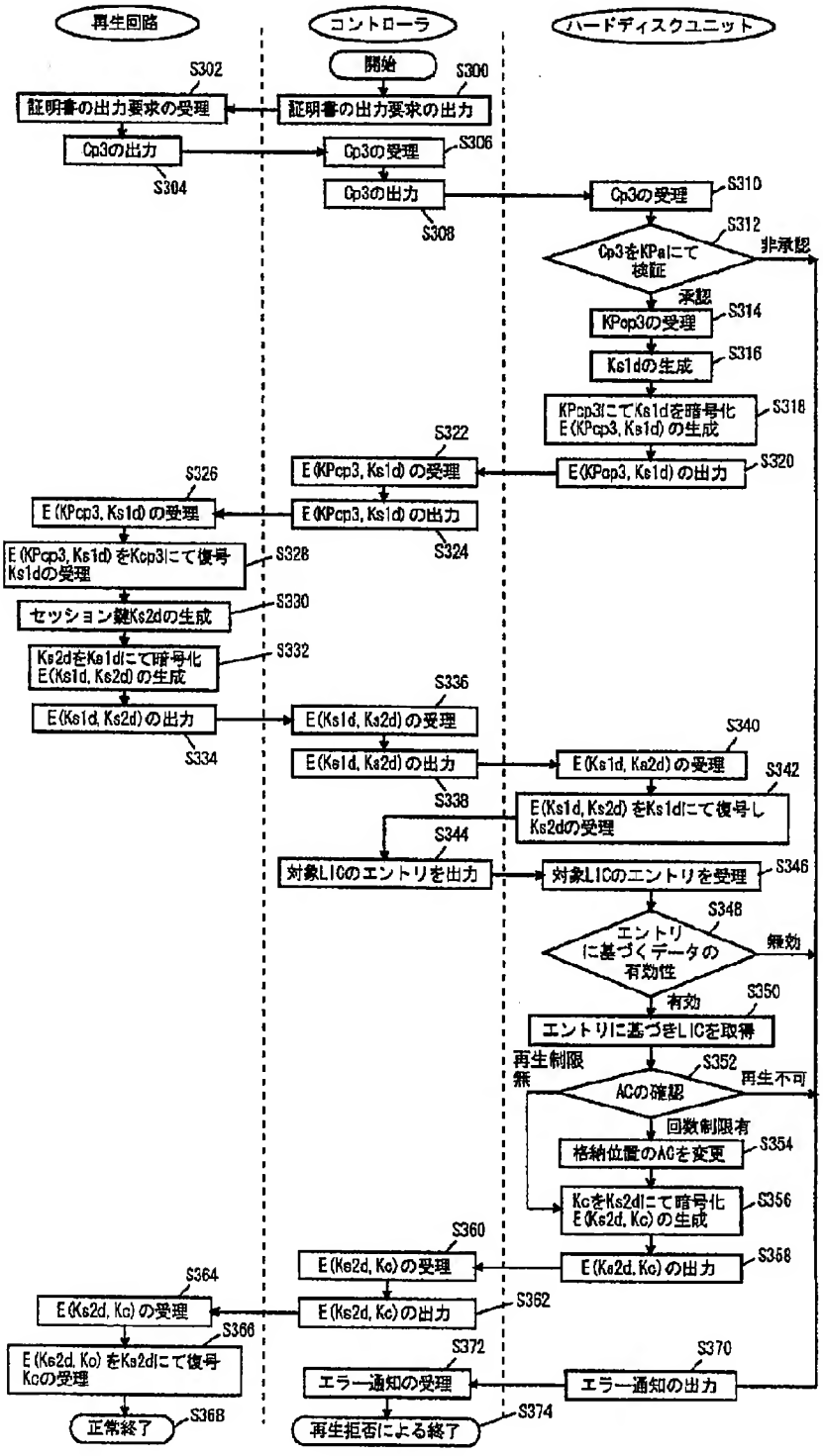
【図１３】


ハードディスクユニット40
端末装置
ハードディスクユニット41
開始
S200
証明書の出力要求の出力
証明書の出力要求の受理
S202
Cm1の受理
S206
Cm1の出力
S204
S210
Cm1の受理
Cm1の出力
S208
S212
Cm1をKPaiにて検証
非承認
承認
KPcm1の受理
S214
Ks1bの生成
S216
S218
KPcm1にてKs1bを暗号化 E(KPcm1, Ks1b)の生成
E(KPcm1, Ks1b)の出力
S220
S222
E(KPcm1, Ks1b)の受理
LID//E(KPcm1, Ks1b)の出力
LID//E(KPcm1, Ks1b)の受理
S226
S224
E(KPcm1, Ks1b)をKcm1にて復号 Ks1bの受理
S228
S230
セッション鍵要求の出力
セッション鍵Ks2bの生成
S232
Ks2bとKPcm4をKs1bにて暗号化 E(Ks1b, Ks2b//KPcm4)の生成
S234
LID//E(Ks1b, Ks2b//KPcm4)の出力
S236
LID//E(Ks1b, Ks2b//KPcm4)の受理
S238
LID//E(Ks1b, Ks2b//KPcm4)の出力
S240
LID//E(Ks1b, Ks2b//KPcm4)の受理
S242
E(Ks1b, Ks2b//KPcm4)をKs1bにて復号し Ks2bとKPcm4の受理
S244
S248
対象LICのエントリを受理
S246
対象LICのエントリを出力
エントリに基づきLICを取得
S250
S252
無効
有効？
有効
S254
LICをKPcm4にて暗号化 E(KPcm4, LIC)の生成
S282へ
S256へ

【図１４】


ハードディスクユニット40
端末装置
ハードディスクユニット41
S212 or S252から
S254から
禁止
S256
ACの確認
複製
移動
S258
エントリに基づくデータの無効化
E(KPam4, LIC)をKs2bにて暗号化 E(Ks2b, E(KPam4, LIC))の生成
S260
E(Ks2b, E(KPam4, LIC))の出力
S262
S264
E(Ks2b, E(KPam4, LIC))の受理
E(Ks2b, E(KPam4, LIC))の出力
S266
S268
E(Ks2b, E(KPam4, LIC))の受理
S270
E(Ks2b, E(KPam4, LIC))をKs2bにて復号 E(KPam4, LIC)の受理
E(KPam4, LIC)をKam4にて復号 LICの受理
S272
S274
LICの格納先エントリを出力
LICの格納先エントリを受理
S276
S278
LIDの一致
一致
不一致
S280
エラー通知の出力
S282
S284
エラー通知の受理
エラー通知の出力
書込拒否による終了
S286
S288
格納先エントリにLICを記録
正常終了
S290

【図１５】


再生回路
コントローラ
ハードディスクユニット
開始
S300
証明書の出力要求の出力
S302
証明書の出力要求の受理
Cp3の出力
S304
Cp3の受理
S306
Cp3の出力
S308
Cp3の受理
S310
Cp3をKPaにて検証
S312
非承認
承認
KPcp3の受理
S314
Ks1dの生成
S316
KPcp3にてKs1dを暗号化 E(KPcp3, Ks1d)の生成
S318
E(KPcp3, Ks1d)の出力
S320
E(KPcp3, Ks1d)の受理
S322
E(KPcp3, Ks1d)の出力
S324
E(KPcp3, Ks1d)の受理
S326
E(KPcp3, Ks1d)をKcp3にて復号 Ks1dの受理
S328
セッション鍵Ks2dの生成
S330
Ks2dをKs1dにて暗号化 E(Ks1d, Ks2d)の生成
S332
E(Ks1d, Ks2d)の出力
S334
E(Ks1d, Ks2d)の受理
S336
E(Ks1d, Ks2d)の出力
S338
E(Ks1d, Ks2d)の受理
S340
E(Ks1d, Ks2d)をKs1dにて復号し Ks2dの受理
S342
対象LICのエントリを出力
S344
対象LICのエントリを受理
S346
エントリに基づくデータの有効性
S348
無効
有効
エントリに基づきLICを取得
S350
再生制限無
ACの確認
S352
再生不可
回数制限有
格納位置のACを変更
S354
KcをKs2dにて暗号化 E(Ks2d, Kc)の生成
S356
E(Ks2d, Kc)の出力
S358
E(Ks2d, Kc)の受理
S360
E(Ks2d, Kc)の出力
S362
E(Ks2d, Kc)の受理
S364
E(Ks2d, Kc)をKs2dにて復号 Kcの受理
S366
正常終了
S368
エラー通知の出力
S370
エラー通知の受理
S372
再生拒否による終了
S374

フロントページの続き

(51) Int. Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ 20/12		Ｇ１１Ｂ 20/12	

Ｆターム(参考) 5B017 AA03 BA07 CA07
5B065 BA01 BA09 PA04 PA16
5D044 BC01 BC08 CC05 CC08 DE03
DE50 EF05 FG18 GK17 HL08
HL11
5J104 AA07 AA12 EA04 KA05 NA03
NA27 NA31